الإرهاب في الفضاء الإلكتروني "دراسة مقارنة"

Cyber Terrorism "a comparative study"

إعداد الطالبة

بدرة هويمل الزبن

إشراف

الدكتور عماد عبيد

مشروع خطة أطروحة دكتوراه فلسفة في القانون العام

كلية القانون-جامعة عمان العربية

2012

التفويض

أنا الطالبه بدره هويمل الزبن أفوض جامعة عمان العربيه بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الأشخاص عند طلبها.

الاسم : بدره هويمل الزبن

التاريخ:2013/7/20

التوقيع: بدره هويمل

قرار لجنة المناقشة

نوقشت هذه الأطروحة وعنوانها: الإرهاب عبر الفضاء الإلكتروني - دراسة مقارنة

وأجيزت بتاريخ: ٥/١٢/٢٠١٢م

الاسم	الصفة	التوقيع
أ.د. عماد محمد ربيع	رئيسا	
عن د. كريمة [illegible] لوجود أطروحتي [illegible]	عضوا	أوقع عن د. كريمة [illegible]
	عضوا	
د. رنا العطور	عضوا	
د. عمار [illegible]	عضوا ومشرفا	٥/٤

الشكر

بعد الحمد، والشكر لله، والصلاة والسلام على سيدنا محمد_صلى الله عليه وسلم_ أتقدم بالشكر الجزيل لأستاذي العزيز الدكتور عماد عبيد الذي أمدني بعلمه وخبرته من أجل إنجاز هذا العمل الذي أتمنى من الله أن يجعل له القبول، فإن أصبت من الله وإن أخطأت فمني.

وأدين بالشكر الى أستاذي فهد الكساسبه الذي ما بخل بعلمه ونصحه.

وإلى كل الذين كانوا السند والعونلي لكل هؤلاء أقول جزاكم الله عنا كل خير.

الاهداء

إلى من أرادت أن أكون وعملت لأكون

إلى أمي أم حتمل ندى إبنه الشهيد ذيب إبراهيم الفلاحات

الى أب أراد الله أن لا أعرفه كإبنه لكنني عرفت سيرته العطره التي لا تزال تملىء حياتنا شرفا وعزه

أبي المرحوم هويمل حتمل الزبن

إلى رفقاء دربي أحبتي و إخوتي

حتمل ومحمد وشمس وأشرف

أهدي هذا العمل

الملخص باللغة العربية

الإرهاب في الفضاء الإلكتروني "دراسة مقارنة"

إعداد الطالبة: بدرة الزبن

اشراف: الدكتور عماد عبيد

تتعلق هذه الدراسة بشكل عام بالإرهاب، تلك الجريمة المعروفة بخطرها وأثرها الكبير على المجتمع وعلى حياة الناس، وقد ظهرت آثارها عبر التاريخ، حيث حصدت أرواح الملايين من الأبرياء، ودمرت مجتمعات، وأشعلت الحروب. هذه الجريمة التي لا تعرف حدود، ولا يوجد في قلوب مرتكبيها رحمة، تلك الجريمة التي لا تميز بين صغير ولا كبير، أو بين ذكر أو أنثى. جريمة لا تقوم على مبدأ ولا دين، وقد تعددت وتطورت صور ارتكابها، وكثر مرتكبيها، وتعددت أهدافهم.

وتبحث هذه الدراسة في واحدة من الصور المستجدة للإرهاب، وهي صورة الإرهاب الإلكتروني. إذ أنه بظهور شبكة الانترنت، وتطور التكنولوجيا في شتى المجالات في العالم، أصبح مرتكبي الجرائم المختلفة يتخذون من وسائل التكنولوجيا الحديثة وسائل جديدة لارتكاب جرائمهم، فظهر كثير من الجرائم التي ترتكب من خلال الإنترنت أو الوسائل الإلكترونية، كما ظهرت أنماط جديدة من الجرائم التي ترتكب ضد هذه الوسائل بذاتها، حيث يكون محل الجريمة وسيلة من وسائل التكنولوجبا والحاسب الآلي.

وكما هو الأمر بالنسبة لمختلف الجرائم التقليدية حيث ظهر مثلها جرائم الكترونية، كالاحتيال الإلكتروني والسرقة عبر الإنترت، فقد ظهر ما يعرف بالإرهاب الإلكتروني، وهذا النمط من الجرائم يعد أساساً جريمة إرهابية بالمفهوم التقليدي، إلا أنه يتم من خلال وسائل تكنولوجية، حيث يقوم الجاني في هذه الجريمة باستخدام الانترنت ووسائل التكنولوجيا الحديثة لارتكاب جريمته أو المساهمة فيها، إما كأداة جريمة، أو أداة تسهل ارتكاب الجريمة، أو تسهل إخفاء آثارها، أو تحقق عناصر الاتصال والتخطيط بين الجناة وغير ذلك من احتمالات. أو قد تكون تلك الوسائل الالكترونية هدفاً للهجمات الإرهابية، بحيث توجه

تلك الهجمات إلى أنظمة المعلومات على الشبكة مثلاً، أو ضد وسائل الاتصال المختلفة، أو ضد أي شيء يعتمد على التكنولوجيا.

وقد بدأت المجتمعات المختلفة تعاني من خطر الإرهاب الإلكتروني، كما عانت في السابق من خطر الإرهاب التقليدي، وبدأت محاولات الحد من هذه الجريمة، أو التخفيف من ارتكابها، وتعددت الجهود التي تقوم بها الدول في هذا المجال، واتخذت صوراً متعددة من النشاط، ومن أهم الأنشطة في هذا المجال، المواجهة القانونية والتشريعية لهذه الجريمة.

حيث تختلف المواقف التشريعية بين الدول في التعامل مع هذه الجريمة، خاصة في ظل عدم وجود تشريعات جنائية كافية تواجه الجرائم المستحدثة، التي ترتكب من خلال وسائل التكنولوجيا أو ضدها، حيث اكتفت بعض الدول بتطبيق النصوص التقليدية في قوانين العقوبات، على تلك الأنماط من الجرائم، وبعض الدول قامت بتعديل تشريعاتها لتواكب مواجهة تلك الجرائم، فأفردت نصوصاً خاصة لمعالجتها، والبعض الآخر أفرد قوانين خاصة لمواجهة جرائم التكنولوجيا الحديثة.

والشيء ذاته ينطبق بالنسبة لجريمة الإرهاب الإلكتروني، إلا أنه وبالمجمل أوضحت الدراسة أن جريمة الإرهاب الإلكتروني، تعد صورة من صور الإرهاب التقليدي، أي أن عناصر الجريمة الإرهابية تتوفر فيها، من حيث الاركان، ومن حيث محل التجريم، وسببه، ومن حيث عنصر الخطر، إلا أنها جرائم ترتكب من خلال وسيلة تكنولوجية أو إلكترونية، أو بمواجهة هذا النوع من الوسائل.

وعليه تقوم هذه الدراسة باستعراض جريمة الإرهاب الالكتروني، بدءً من التعريف بجريمة الإرهاب التقليدي، والتعرف على أسبابه، وأشكاله، وأركان الجريمة، وصورها، ثم بيان العلاقة بين الفضاء الإلكتروني والجريمة المعلوماتية، وبين الإرهاب. وفي هذا المجال توضح الدراسة النشاط الجرمي المكون للركن المادي في جريمة الإرهاب الإلكتروني، وتبحث في الركن المعنوي لهذه الجريمة، الذي لابد من توافره كما هو الأمر بالنسبة لأي جريمة أخرى.

كما تهدف الدراسة الى البحث في طرق مكافحة الإرهاب الإلكتروني، لهذا فإنها تبحث في الصعوبات القائمة، أو التي قد تظهر في مجال مكافحة الإرهاب الإلكتروني، وتعمل على التوصل لبعض

التدابير اللازمة للحماية منها. وهذا الأمر استدعى الحديث عن الجهود الدولية في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني، سواء على مستوى الجهود الإقليمية، أو الجهود الوطنية في مجال مكافحة الإرهاب التقليدي أو الإلكتروني.

وبشكل عام تتوصل الدراسة إلى أن هناك صورة جديدة من صور الأعمال أو الجرائم الإرهابية، تتخذ من وسائل التكنولوجيا أداة لارتكابها، وإما أن تكون الوسائل الإلكترونية هدفاً لتلك الأعمال أو الجرائم. وأنها تتشابه كثيراً مع الجرائم الإرهابية التقليدية.

كما أنها تستخدم كافة الوسائل المتاحة في المجال الإلكتروني، كالبريد الإلكتروني، والمواقع الإلكترونية، ووسائل الاتصالات المختلفة، ومواقع التواصل الاجتماعي، وغرف الدردشة، وذلك من حيث ممارسة بعض الأنشطة الإرهابية، كالاتصالات، والتدريب، ونشر المعلومات التي تتضمن طابع التهويل والتخويف. كما أنها تستخدم بعض وسائل التدمير والتفجير في المجال الإلكتروني، كالإغراق بالرسائل، وزرع الفيروسات، والقنابل الإلكترونية، وحصان طروادة، وغير ذلك من وسائل.

وفي مجال مكافحتها، عالجت الدراسة بعض الاتفاقيات، التي إما أن تصب في إطار الإرهاب والأعمال الإرهابية بشكل عام، أو في إطار الإرهاب الإلكتروني، وذلك إلى جانب بعض التشريعات التي تتعلق بهذا الأمر أيضاً، والتي منها القانون المؤقت لجرائم أنظمة المعلومات الأردني الجديد.

الملخص باللغة الانجليزية

Abstract

Cyber Terrorism "a comparative study"

Prepared by: Alzaben Badra

Supervised by: Dr. Obeid Emad

This study relates generally to the terrorism, that crime which is known by its danger, and its big impact on society and on people's lives. Its effects have appeared throughout history, which caused the death of millions of innocent people, destroyed communities, and ignited wars. This crime knows no boundaries, and no mercy in the hearts of the perpetrators, and do not distinguish between old or young, or between a male and female. A kind of crime which is not based on principle or religion, it has varied and evolved ways to commit, and many perpetrators, and numerous goals.

This study examines one of the emerging ways of terrorism, the cyber-terrorism, By the appearance of the Internet, and the evolution of technology in various areas in the world, perpetrators have become using new technology to execute their crimes, which led to emerge various crimes that committed through the Internet or electronic means, also new types of crimes committed against these means itself appeared.

As the case for the various traditional crimes which appeared, new electronic crimes similar to them, for example, phishing and theft across internet. this happened to terrorism where emerged what is known as cyber-terrorism, This type of crime is primarily a terrorist crime in the traditional sense, but it is done through technological means, where the offender in this crime uses the Internet and modern technology to commit crime or contribute, either as a crime, or a tool to make the commission of the crime, or to reduce concealment effects, or to check the elements of communication and planning between the perpetrators and other possibilities. Or it may be that electronic means target for terrorist attacks, so they attack for example, information systems on the network, or attack the various means of communication, or anything that depends on technology.

Various communities have begun to suffer from the threat of cyber-terrorism, as suffered in the past the threat of traditional terrorism, so it began their efforts to forbid this kind of crimes or reduce it through many ways, and one these important effort is the legal and legislative confrontation.

These legislative positions are different among countries in dealing with this crime, especially in the absence of criminal legislation adequate to face emerging crimes which committed by means of technology or against it, where some countries use the texts of their traditional penal laws to treat with those types of crimes, and other countries has amended its legislation to keep pace with the face of such crimes so it singled out special provisions to address it, while others singled out special laws to address the crimes of modern technology.

The same thing applies for the crime of cyber–terrorism, but the study showed that the crime of cyber–terrorism is one of traditional terrorism crime, that the elements of terrorism crime is available, in terms of staff, and in terms of place of criminality, and why, and where the element of risk, but as crimes committed through the through technological or electronic means, or against this means.

Therefore, this study reviews the crime of cyber–terrorism, from the traditional definition of the crime of terrorism, and it identifies the causes, forms, elements of the crime, and its images, then the statement of the relationship between cyberspace and cyber crime, and terrorism. In this regard, the study clarifies activities and components of the crime, as a physical element in the crime of cyber–terrorism, and looking at the mental element of the crime, which must be available as it is in the case for any other crime.

The study aims to look at ways to combat cyber-terrorism, so they are looking at the current difficulties, or that may appear in the fight against cyber-terrorism, and work to reach some of the measures necessary to protect their communities . This led to talk about international efforts to combat traditional terrorism and cyber-terrorism, both at the level of regional efforts, or national efforts.

In general, the study shows that there is a new way in terrorist crimes, take the means of technology is a tool to commit, or electronic means to be the target of such acts or offenses. And, they are very similar with traditional terrorist crimes.

It also uses all available means in the field of cyber space, such as e-mail, websites, means of various communication, social networking sites, and chat rooms, and in terms of the practice of some terrorist activities, such as communications, training, and dissemination of information which includes the nature of exaggeration and intimidation. It also uses some of the means of destruction and bombings in the field of electronic communications; Flooding messages, planting viruses, and e-bombs, Trojan horses, and other means.

In the area of counter cyber crimes, the study addresses some of the agreements, which is discharged into the framework of terrorism and terrorist acts in general, or in the context of cyber–terrorism, and also some of the legislation concerning this matter as well, such as the new temporary Jordanian law for information system Crimes.

الفهرس

الفصل الاول

الإطار العام للدراسة

أولاً: المقدمة

الإرهاب الإلكتروني يعني ببساطة استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية، أو استخدام الفضاء الإلكتروني في تنفيذ وتسهيل تنفيذ الهجمات الإرهابية[1] وعرفه آخرون بأنه:" العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الإنسان: بدينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق، بشتى صنوفه وصور الإفساد في الأرض" [2]. والذي كان ولا زال مثار جدل من حيث وضع تعريف جامع مانع له، وكل ما بذل هو محاولات للتعريف. ، إلا أن أهم ما يميز الإرهاب الإلكتروني عن الإرهاب بمفهومه العام هو نوعية الأداة المستخدمة لتحقيق الغرض الإرهابي، أو الشيء المستهدف من العمل الإرهابي الذي قد يكون الفضاء الإلكتروني بالنسبة للإرهاب الإلكتروني، إذ أنه يعتمد على استغلال الإمكانيات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

وهو كالإرهاب بمفهومه العام يقوم على العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية، وقد يرتكب من قبل الدول أو الجماعات أو الأفراد على السواء، وهو يقع على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله من خلال استخدام التقنيات الرقمية.

وحول تعريف الإرهاب بشكل عام نجد اهتمام الامم المنحدة منذ نشأتها بتعريفه، حيث عرفته أنه تلك الأعمال التي تعرض للخطر أرواحاً بشرية بريئة أو تهدد الحريات الأساسية أو تنتهك كرامة

---

1 عرفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937 الإرهاب أنه:"الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة".

2 السند، 2004م، ص8 .

الإنسان(الكيلاني، 1997، ص17). وعلى المستوى العربي عرفته الاتفاقية العربية لمكافحة الإرهاب لعام 1998 أنه:"كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر". كما يعرف الإرهاب بموجب القانون الدولي أنه جملة من الأفعال التي حرمتها القوانين الوطنية لمعظم الدول(الكيلاني، 1997، ص51).

وللإرهاب الإلكتروني خصائص تميزه عن الإرهاب بمفهومه العام أهمها ما ينبع عن خطورة الفضاء الإلكتروني ذاته، حيث أن الإرهابي الإلكتروني لا يترك أي دليل مادي بعد ارتكاب جرائمه، مما يجعل عملية تعقبه واكتشافه أمراً صعباً للغاية، كما يتميز بسهولة إتلاف الأدلة في حال العثور عليها، كما يمتاز مرتكبيه بتمتعهم بخبرات في استخدام الأجهزة والتقنيات الحديثة مقابل نقص الخبرة لدى الجهات الأمنية المسؤولة عن كشف المخططات الإرهابية الرقمية، كما أن الإرهاب الإلكتروني يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة، وكل ما يحتاجه عباره عن جهاز حاسب آلي وبعض البرامج وشبكة إنترنت، وعلى الغالب الاعم تتم العمليات الإرهابية بتعاون عدة أشخاص مع بعضهم البعض تحت ما يعرف بالمنظمات الإرهابية، علماً بأن أهم ما يميز هذا النوع من الإرهاب هو أنه ليس إرهاباً بذاته إنما هو وسيلة لتسهيل تنفيذ العمليات الإرهابية.

ولهذا النوع من الإرهاب مظاهره وأشكاله، فقد يتم من خلال تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، وقد يتم من خلال إنشاء المواقع الإرهابية الإلكترونية، أو من خلال تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، أو بالتهديد والترويع الإلكتروني، أو بالتجسس الإلكتروني.

ويواجه العالم اليوم تطوراً هائلا في وسائل الاتصالات وتقنية المعلومات، حتى أصبح يطلق عليه عصر الثورة المعلوماتية، التي ساهمت في ظهور هذا النوع من الإرهاب، وشيوع إستخدامه، الأمر الذي زاد من خطورته، فهو يقوم عى استغلال موارد العالم المادي والإفتراضي، من خلال الوصول إلى المداخل العامة والخاصة بين العالمين، والإنتقال والتجمع، لتدمير نقاط الإلتقاء الإيجابية التي تمثل حالة للرفاه المجتمعي والمعرفي، ويعمل على خلق تغييرات جوهرية في الأنظمة العاملة وتدمير البنية

المعلوماتية التحتية للخصوم والأعداء خاصة ما يتعلق منها بالقوات المسلحة وتـدمير أنظمـة الإتـصال الجوية والبرية والبحرية وذلك من خلال إستخدام تقنية المعلومات.

وقد دعا ذلك دول العالم إلى الدخول في اتفاقيات دولية لمكافحته فكانت أول إتفاقية دولية لمكافحة الإجرام المعلوماتي في العاصمة المجرية بودابست عام 2001، عقب الهجمات الإرهابية التي تعرضـت لها الولايات المتحدة الأمريكية في الحادي عشر من سبتمبر من العام نفسه.

ومما يؤكد الخطورة الكامنة في هذا النوع من الإرهاب اعتماد الدول بشكل كبير الآن على وسائل الإتصالات وشبكات المعلومات، مما فتح المجال أمام الإرهابيين لتحقيق أهدافهم وتدمير منتجات التقنيـة الحديثة والتي تخدم الإنسانية وتسهل التواصل المعرفي والعلمي والثقافي، فباتت المعلومات في هذا القرن عرضة لكافة المخاطر المحتملة من هذا النمط المتجدد من الإرهاب المعاصر.

كما أن تقنية المعلومات تسهل ارتكاب الجرائم الإرهابية، فتسهل إلتقاء الإرهـابيين والمجـرمين الذين يصعب عليهم الالتقاء في الحياة المادية العادية، فيلتقون على الشبكة لتعلم طرق الإجرام والإرهاب وتبادل الآراء والأفكار والمعلومات والأحاديث والإستماع لبعضهم عبرها، كما أنها تسهل علـيهم نـشر أفكارهم ومبادئهم باستخدام تقنيات الانترنت المختلفة كالمنتديات وغرف الحوار الإلكترونيـة، والبريـد الإلكتروني ومواقع التواصل الاجتماعي.

وتسهل هذه التقنيات لمرتكبي الإرهاب الإلكتروني بيئة خصبة لممارسة جرائمهم لأنهـا تـسهل عليهم نشر أفكارهم الهدامة وتحقيق أهدافهم السيئة، ولأنها تمتاز بوفرة المعلومات الموجودة فيها، فتعـد موسوعة إلكترونية شاملة متعددة الثقافات، ومتنوعة المصادر، وغنية بالمعلومات الحساسة التي يـسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيـادة والـسيطرة والإتصالات ومواعيد الرحلات الجوية الدولية، والمعلومات المختصة بسبل مكافحة الإرهاب، ونحو ذلك من المعلومات التي تعتبر بمثابة الكنز الثمين بالنسبة للإرهابيين، نظراً لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية. كما يسهل الانترنت العمليات الإرهابية لأنها تعد عمليات على جانب من التعقيد

والصعوبة، وتحتاج للتخطيط المحكم والتنسيق الشامل، حيث يعد وسيلة إتصال بالغة الأهمية للجماعات الإرهابية.

كما تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح بعيداً عن أعين الناظرين، ويمكنهم من ترتيب تحركاتهم، وتوقيت هجماتهم والإستعانة بالبيانات الإحصائية السكانية المنتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية، من خلال الإستفسارات والإستطلاعات الموجودة على المواقع الإلكترونية، حيث يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة، والقلوب الرحيمة، ومن ثم يتم إستجداؤهم لدفع تبرعات مالية لأشخاص إعتباريين يكونون واجهة لهؤلاء الإرهابيين.

كما يعد الانترنت وسيلة مناسبة لتلك الجماعات لتلقي تدريباتها، اذ يمكن استخدام الانترنت لأغراض التدريب على وسائل الاتصال وتنفيذ الهجمات الإرهابية والتخطيط لها ونشر المعلومات التدريبية وتبادلها من خلال الشبكة وتطبيقاتها.

إن هذه الخصائص والمزايا التي ميزت الانترنت وميزت الجرائم التي ترتكب من خلاله خاصة جرائم الإرهاب، ولخطورة هذه الجرائم وأهميتها سواء أرتكبت بوسيلة إلكترونية أم وسيلة تقليدية فإنه اصبحت تستقل بمفهوم خاص بها، وهو ما يعرف بالإرهاب الإلكتروني مضمون وموضوع دراستنا هذه. ولهذا الإرهاب كنوع جديد أو وسيلة جديدة من وسائل ارتكاب الجرائم والهجمات الإرهابية دوافعها الخاصة وأهدافها المستقلة إلى جانب الأهداف المبتغاة من الإرهاب التقليدي، وهذه الأهداف أيضاً لها أسبابها ولها أسباب أخرى جعلتها تلجأ إلى استخدام الوسائل الإلكترونية في تنفيذ هجماتها واستخدام الانترنت فيها.

ومتى تم استخدام الانترنت والفضاء الإلكتروني لتنفيذ الهجمات الإرهابية أو التخطيط لها أو المساهمة باي شكل من الاشكال في تنفيذ الهجمات الإرهابية فإن ذلك يعكس صوراً متعددة للاعتداءات التي يمكن أن تتم من خلاله، اذ يمكن القول أن للإرهاب الإلكتروني صوراً ومظاهر واشكال. وهذه الصور بجميعها لابد من ايجاد الوسائل اللازمة لمكافحتها ومقاومتها وحماية المجتمع منها.

بالتالي فإن تناول موضوع الإرهاب الإلكتروني أو إرهاب الفضاء الإلكتروني كما هو في دراستنا يحتاج التعرف على مفهومه وأسبابه وخصائصه ومظاهره، والتعريف بالجريمة الإلكترونية بشكل عام وعلاقتها بالإرهاب الإلكتروني. والتعرف قدر الإمكان على دور البيانات والمعلومات في جرائم إرهاب الفضاء الإلكتروني، وكيفية ارتكابها من خلال الفضاء الإلكتروني.

أما الجانب الاهم في دراستنا فيأتي في التعرف على آلية مكافحة هذه الجرائم والتصدي التشريعي لها، وهذا يحتاج التعرف على الإطار التشريعي لها في التشريع الأردني، ومقارنته قدر الإمكان بالتشريعات الأخرى، للتعرف على مدى فاعلية التشريعات خاصة الحديثة منها في مواجهة جرائم الإرهاب الإلكتروني.

ثانياً: مشكلة الدراسة

تدور مشكلة الدراسة حول ظهور نوع جديد من جرائم الإرهاب وهي جرائم الإرهاب الإلكتروني ، والتي تتم من خلال استخدام الانترنت وتطبيقاته المختلفة، وهي جرائم تتسم بالخطورة لسهولة ارتكابها والتخطيط لها وتدريب الجناة فيها ونشر معلوماتها، وتحقيق الاتصال فيما بينها بسرعة وسهولة فائقة لأنها تستفيد من خدمة تقنية الانترنت وتطبيقاتها وما تمتاز به من سهولة الاستخدام وخصوبة ووفر المعلومات اللازمة لمرتكبي هذه الجرائم.

بالتالي فإن الغرض من هذه الدراسة هو التعرف على الإرهاب في الفضاء الإلكتروني من حيث ماهيته وخصائصه، وسمات مرتكبيه، ووسائل ارتكابه، وأركانه، والنتائج التي يفضي إليها، والتعرف على طرق مكافحته، والتأكد من مدى كفاية التصدي التشريعي له.

ثالثاً: عناصر مشكلة الدراسة

تحاول هذه الدراسة الإجابة عن الأسئلة التالية:

1. ما هو مفهوم الإرهاب الإلكتروني وأسبابه وخصائصه ومظاهره؟
2. ما هي الجريمة الإلكترونية وعلاقتها بالإرهاب الإلكتروني؟
3. كيفية ارتكاب جرائم الإرهاب من خلال الانترنت وتطبيقاته؟
4. ما هو دور البيانات والمعلومات في هذه الجرائم؟
5. كيف يتم التهديد والترويع في الإرهاب الإلكتروني؟
6. ما هي صور وأشكال الإرهاب الإلكتروني الذي قد يتم من خلال الانترنت؟
7. ما مدى فاعلية وكفاية التشريعات القائمة في مواجهة جرائم الإرهاب الإلكتروني؟
8. ما هو الإطار التشريعي لهذه الجرائم في التشريع الأردني والتشريعات الأخرى؟

رابعاً: أهمية الدراسة

تظهر أهمية الدراسة كالآتي:

أ. محاولة إستكشاف وتحديد معالم ظاهرة الإرهاب الإلكتروني التي تقوم على إستخدام الإنترنت وتطبيقاته المتعددة كالبريد الإلكتروني والمنتديات وغرف الدردشة ومواقع التواصل الاجتماعي، وهي المواقع التي نستخدمها في حياتنا اليومية بشكل كبير، والتي نعرض أنفسنا وابناءنا لها مما يجعلنا عرضة لأن نكون مستهدفين للاستدراج والانخراط في تلك الجماعات التي تسعى جاهدة لاستقطاب أكبر شريحة من المجتمع لدعم قوتها ومكانتها.

ب. التعرف على هذه الجرائم وأساليبها وصورها وأشكالها ومرتكبيها وسماتهم والطرق والأساليب التي يستخدمونها لارتكابها.

ت. التعرف على أركان هذه الجرائم ومقارنتها بجرائم الإرهاب التقليدي.

ث. تحديد مفهوم هذه الجرائم وإبراز معالمها لكافه أفراد المجتمع وتعريف المجتمع بأن هذه الطائفة من الجرائم تحتوي على مخاطر جمة لا يمكن حصرها خاصة وانها في حالة تطور مستمر، وتتطور بتطور تقنيات الانترنت وتطبيقاته. وتعريف الناس بحجم الخسائر الناتجة عن هذه الجرائم كونها لا تستهدف الأفراد فقط بل تستهدف الدول، وتعتدي على البيانات والمعلومات والبرامج بكافة أنواعها، كما أنها تستخدم هذه المعلومات لتحقيق أهدافها بالتالي فإنها قد تعترض المعلومات المنقولة عبر نظام شبكات الإنترنت وتتمكن من اختراق أنظمة الحماية للحصول عليها.

ج. تتمثل أهمية الدراسة بخطورة هذه الجرائم التي تمس حياة الفرد الخاصة وتهدد الأمن القومي وسيادة الدولة على السواء، وتتسبب بفقدان الثقة بالتقنية الإلكترونية وابداع العقل البشري.

خامساً: أهداف الدراسة

تهدف الدراسة إلى:

1. التعرف على مفهوم هذه الجرائم وتحديد طبيعتها القانونية.
2. البحث في أركان هذه الجرائم وأساليبها وصورها ومظاهرها والنتائج التي قد تفضي إليها.

3. البحث في الإطار التشريعي لهذه الجرائم في التشريعات الجنائية الأردنية وبيان مدى كفايتها وتحقيقها للردع في هذا المجال.
4. تحديد الإختصاص القضائي لنظر هذه الجرائم، وإمكانية إجراء التحقيق فيها كما هو الحال بالنسبة للجرائم التي ترتكب بالوسائل التقليدية.
5. تهدف الدراسة إلى المساهمة في محاربة ومكافحة جرائم الإرهاب الإلكتروني من خلال الوسائل الوقائية ووضع الدراسات اللازمة لبيان كل ما يتعلق بهذه الجرائم، وانتهاء إلى وضع تشريع خاص بهذه الجرائم يحقق القدر الأكبر من الفائدة في مجال مكافحتها، خلافاً لما هو الحال في النصوص المبعثرة.
6. نشر الوعي بين الأفراد والتحذير من تلك الإعتداءات الناتجة عن هذه الجرائم.

سادساً: منهج الدراسة

ستقوم الباحثة باستخدام المنهج الوصفي والمنهج التحليلي والمنهج المقارن على النحو التالي:

أ. المنهج الوصفي

من خلال وصف جرائم الإرهاب الإلكتروني وتعريفها وبيان آلية ارتكابها ودور التكنولوجيا وتطبيقات الانترنت فيها وكيفية استخدامها لتحقيق هذه الغاية، ووصف أركان الجريمة وبيان عناصرها ونتائجها، ومن ثم وصف الطرق اللازمة لمكافحتها والتقليل منها.

ب. المنهج التحليلي

وذلك بتحليل الكتب والوثائق والنصوص القانونية الواردة في التشريعات المختلفة وفي الوثائق الدولية من معاهدات ومؤتمرات وغيرها للوصول إلى أهداف الدراسة.

ج. المنهج المقارن

وهو المنهج الذي يقوم على إجراء المقارنات اللازمة بين التشريعات الأردنية المختلفة في مجال جرائم الإرهاب والعقاب عليها مع غيرها من التشريعات الحديثة في هذا المجال.

سابعاً: محددات الدراسة

تتعلق هذه الدراسة بالإرهاب الإلكتروني أي بالإرهاب الذي يتم من خلال استخدام وسائل التكنولوجيا الحديثة المتمثلة بالانترنت وتطبيقاته المختلفة، أو الإرهاب الذي يستهدف هذه التقنيات، أو يستخدمها لترويع وتخويف الآخرين. بالتالي فإنها لا تتعلق بالإرهاب التقليدي ولن تتطرق إليه إلا من باب المقارنة وتحقيق الفائدة للدراسة واضفاء طابع الشمول عليها.

كما تتعلق هذه الدراسة بالنصوص القانونية الواردة في قانون جرائم نظم المعلومات المؤقت لسنة (2010) والنصوص الواردة في قانون العقوبات الأردني فيما يتعلق بجريمة الإرهاب الإلكتروني، الا في الحالات التي تقتضي الدراسة الرجوع على غيرها من التشريعات ومقارنتها بالتشريعات الأخرى.

ثامناً: فرضيات الدراسة

لقد قامت هذه الدراسة على عدة افتراضات وهي:

1. عدم وجود لنصوص تشريعية واضحة وكافية لتغطية هذا النوع من الجرائم. وعدم وجود لقانون واضح المعالم يتعلق بهذه الطائفة من الجرائم.
2. تتحقق جرائم الإرهاب الإلكتروني من خلال استخدام الانترنت بكافة تقنياته، كما أن الانترنت بذاته قد يكون هو الهدف من هذه الجرائم. كما أنه قد يستخدم لإخافة وترويع الآخرين.

3. تقوم المسؤولية الجزائية وتثبت عن ارتكاب هذه الجرائم من خلال التلاعب المقصود وغير المشروع بالبيانات والوسائل الإلكترونية.

تاسعاً: التعريفات الإجرائية

من أهم المصطلحات التي سوف ترد خلال هذه الدراسة :

- الإرهاب: تعرف الجمعية العامة للأمم المتحدة في المادة 193 من إتفاقية جنيف الإرهاب أنـــه:" كافـــة الأفعال الإجرامية ضد دولة من الدول التي من شأنها بحكم طبيعتها أو هدفها إثارة الرعب فـــي نفـــوس جهات معينة أو جماعات من الأشخاص لأهداف سياسية غير مبررة تحت أية ظروف ومهما بلـــغ مـــن حالات سياسية أو دينية أو عرقية".

- الشبكة المعلوماتية (الإنترنت): عبارة عن إرتباط دائم بين أكثر من نظام معلومات للحـــصول علـــى البيانات وتبادلها.

- الموقع الإلكتروني: عبارة عن مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

- المعلومات: وهي البيانات التي تمت معالجتها وأصبح لها دلالة واضحة.

- البرامج: عبارة عن مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ بإســـتخدام أنظمه المعلومات.

- نظام المعلومات: عبارة عن مجموعة من البرامج والأدوات المعدة لإنـــشاء البيانـــات أو المعلومـــات إلكترونياً، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها.

- البيانات: هي الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها.

- التصريح: هو الإذن الممنوح من صاحب العلاقه إلى شخص أو اكثر للدخول إلى أو إستخدام نظـــام المعلومات أو موقع إلكتروني أو الشبكه المعلوماتيه بقصد الإطلاع أو إلغاء أو حذف أو إضافه أو تغييرأو إعاده نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزه أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته.

عاشراً: الدراسات السابقة

من خلال البحث تبين وجود بعض الدراسات المشابهة نوعاً ما وذات الصلة بموضوع دراستنا وتبينها الباحثة كالآتي:

1- دراسة يونس عرب (جرائم الحاسوب)، دراسة مقارنة 1994.

تتعلق هذه الدراسة بمفهوم عام وهو جرائم الحاسوب، وتحديد الأفعال الجرمية التي تدخل في نطاقها، وتعمل على تحليلها في ضوء محددات نصوص التجريم التقليدية في قوانين العقوبات بشكل عام، وقانون العقوبات الأردني بشكل خاص، وتحديد مدى قابلية هذه النصوص للإنطباق على هذه الأفعال التي ترتكب من خلال الحاسب الآلي. إلا أنها لم تتطرق لدراسة الجرائم الإرهابية الإلكترونية باعتبارها من الجرائم التي ترتكب من خلال الحاسب الآلي لأن الانترنت لا يتم إلا من خلال الحاسب الآلي ذا المفهوم العام.

وذلك بخلاف دراستنا التي تتعلق ابتداء بجرائم الإرهاب الإلكتروني ولا تتطرق لأي جريمة من الجرائم الأخرى التي ترتكب من خلال الحاسب الآلي.

2- دراسة أبوغليون بعنوان: الجرائم الإلكترونية مقارنه بين الشريعة والقانون، 2009.

وتتعلق هذه الدراسة أيضاً بالجرائم الإلكترونية فقط وبشكل عام، واوصت بالعمل على المحافظة على البرامج الإلكترونية لما لها من أهمية في تيسير الحياة البشرية، وأهميتها الاقتصادية، وقامت بالتعريف

بالجرائم الإلكترونية واضرارها، وكيفية حماية البرامج الإلكترونية من الاعتداء عليها واستهدافها دون الاشارة إلى جريمة الإرهاب الإلكتروني.

3- دراسة العتيق بعنوان: الجرائم الإلكترونية والادلة الجنائية الإلكترونية، 2010.

وقد تناولت هذه الدراسة تعريف الجريمة الإلكترونية والدوافع العامة لارتكابها، وثم تناولت اوصاف مرتكبي هذه الجرائم بالاضافة إلى تصنيف الجريمة الإلكترونية ووسائل الحماية منها والعقوبة المفترض تنفيذها حسب المشرع السعودي. ثم تناولت بشكل يسير مفهوم الإرهاب وانواعه، إلا انها لم تتطرق لمفهوم الإرهاب الإلكتروني، وموقف المشرع الأردني والتشريع المقارن منه. كما أنها تعلقت بالنسبة للجريمة الإلكترونية بموقف المشرع السعودي فقط.

4- دراسة السند بعنوان: وسائل الإرهاب الإلكتروني، حكمها في الإسلام وطرق مكافحتها، 2010.

تمثل هذه الدراسة رسالة جامعية، وقد ارتكزت على توضيح وسائل ما يعرف بالإرهاب الإلكتروني، وأكدت على أن التقنية الحديثة غير قادرة وحدها على حماية الناس من الأعمال الإرهابية عبر الانترنت التي باتت تشكل هاجساً يؤرق العالم في كل مكان، وارتكزت الدراسة على أهم المخاطر الناتجة عن هذا النوع من الإرهاب، وتوضيح ماهيته وحكمه في الشريعة الاسلامية، وكل ذلك من وجهة نظر إسلامية.

أما بالنسبة لدراستنا فإنها لم تقف عند حد وسائل الإرهاب الإلكتروني عبر الانترنت، ولم تتحدث عن موقف الشريعة الاسلامية منه، إلا انها تعالج كل ما يتعلق بالإرهاب الإلكتروني، من خلال وجهة نظر المشرع الأردني وبعض التشريعات المقارنة بالنسبة لهذه الجرائم، والجهود الدولية لمكافحتها.

5- دراسة العفيف حول: جرائم الإرهاب في قانون العقوبات الأردني، 2011.

تناولت هذه الدراسة موضوعات قانونية على المستوى الوطني والدولي بالنسبة لجرائم الإرهاب، وكما وردت في قانون العقوبات الأردني، ولفت الباحث فيها النظر إلى أن المشرع الأردني بحاجة للنص على أحكام خاصة جديدة لمواكبة هذا النوع المتطور من الإرهاب. الا أن الدراسة برمتها تركز على الإرهاب بمفهومة التقليدي.

وذلك بخلاف دراستنا التي تتناول الإرهاب الذي يتم من خلال الفضاء الإلكتروني، وتركز على موقف المشرع الأردني في قانون العقوبات الأردني، والى الجهود الدولية للحماية من هذه الجرائم ومكافحتها، وعلى المستوى الدولي.

6- دراسة الزنط بعنوان: الإرهاب عبر الانترنت أخطر من الحرب الباردة، 2011.

تناولت هذه الدراسة استخدام الانترنت كطريقة لتحقيق جرائم الإرهاب الإلكتروني، الذي خـــرج بوضوح أكبر بعد عمليات الحادي عشر من سبتمبر الشهيرة، وأشارت الدراسة إلى أن هذا النـــوع مـــن الجرائم له صفة سياسية، ويسعى لتحقيق أهداف متعددة، تؤثر بشكل أكبر على الجانب المعنوي والنفسي للمجتمعات، وقدمت تعريف شامل للإرهاب الإلكتروني عبر الانترنت. وتوصلت الدراسة إلى أن العديـــد من الدول مثل أمريكا وفرنسا واليابان وتايوان وماليزيا، قد وضعت قوانين وتشريعات لحماية نفسها مـــن خطر الإرهاب الإلكتروني، وذلك من خلال المراقبة للمواقع الخطرة بالانترنت. وتتشابه هذه الدراسة مع دراستنا في الكثير من جوانبها، إلا أنها تركز على مفهوم الإرهاب وربطه بمفهوم الحرب الباردة.

إلا انها تختلف عن دراستنا كون دراستنا تركز على الجانب الإلكتروني الذي قد يكـــون وســـيلة لارتكاب الجرائم الإرهابية وقد يكون أداة لتهديد الآخرين وإشاعة الذعر بينهم، كما أنها قد تكون غايـــة، وكل ذلك يختلف من واقعة لأخرى ومن جريمة لأخرى، وحسب الدوافع لارتكاب الجرائم الإرهابية، التي قد تكون لدوافع سياسية أو اقتصادية أو أمنية، كما تقوم دراستنا على البحث في موقف التشريع الأردنـــي من هذه الجرائم ومدى كفايته، مقارنة بنظرة التشريع المقارن، كما تبحث في الجهود الدولية فـــي مجـــال مكافحة هذه الجرائم والتصدي التشريعي الكافي واللازم لها.

حادي عشر: مخطط الدراسة

الفصل الاول: الإطار العام للدراسة

الفصل الثاني: ما هية الإرهاب الإلكتروني

المبحث الاول: ما هية الإرهاب التقليدي وأسبابه

المبحث الثاني: الفضاء الإلكتروني وعلاقته بالإرهاب والجريمة المعلوماتية

المبحث الثالث: التعريف بالإرهاب الإلكتروني وحرب المعلومات

الفصل الثالث: أركان جريمة الإرهاب الإلكتروني وأشكالها

المبحث الاول: النشاط الجرمي المكون للركن المادي في جريمة الإرهاب الإلكتروني

المبحث الثاني: الركن المعنوي في جريمة الإرهاب الإلكتروني والعقاب عليها

المبحث الثالث: صور وأشكال الجرائم الإرهابية في الفضاء الإلكتروني

الفصل الرابع: مكافحة الإرهاب الإلكتروني

المبحث الأول: الصعوبات والتدابير في مجال مكافحة الإرهاب الإلكتروني

المبحث الثاني: الجهود الدولية في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

المبحث الثالث: الجهود الإقليمية والوطنية في مكافحة الإرهاب

الفصل الخامس: الخاتـــــــمة والتوصيات

الفصل الثاني

ما هية الإرهاب الإلكتروني

من المعروف أن الجرائم تتفاوت فيما بينها من حيث جسامتها وخطورتها، بما في ذلك جريمة الإرهاب، كما تتفاوتت التشريعات في طريقة تبنيها ومعالجتها لأحكامها، تبعاً لاختلاف مفاهيمها عنها وتعريفها لها. إلا أنه بات من المستقر أن جميع الدول تجرم الإرهاب استناداً لعنصر الخطر أو ما يعرف بالترويع والتخويف الذي ينصب على المجني عليه بسبب ارتكاب هذه الجريمة.

وتتم هذه الجريمة بعدة أشكال وصور، حتى يمكن القول أنها تتكون من مجموعة معينة من الأفعال تعد بحد ذاتها جرائم مستقلة بذاتها إن ارتكبت بشكل فردي بعيد عن عنصر الترويع والتخويف الذي يلازم السمة الإرهابية. إلا أن هذه الأعمال تجرم تحت وصف جرمي جديد هو جريمة الإرهاب.

كما أن التطور الحاصل في مفاهيم الحياة ومعطياتها، والتقدم التكنولوجي بشتى مجالاته، قد تسبب بتطور الحياة الاجتماعية معه، وأدى إلى تبدل في كثير من المفاهيم وأساليب وأنماط الحياة بما في ذلك أنماط الجرائم، وتسبب بظهور أنواع جديدة من الجرائم، كما أصبح بالامكان ادخال هذه التكنولوجيا في طرق ارتكاب الجرائم، حتى باتت وسيلة مساعدة ومسهلة لارتكاب بعض أنواع الجرائم. ومن هذه الجرائم الحديثة جريمة الإرهاب الإلكتروني أو الإرهاب في الفضاء الإلكتروني محور دراستنا.

وللوقوف على حيثيات هذه الجريمة وأحكامها وطرق مكافحتها والوقاية منها، كان لزاماً التعريف أولاً بالإرهاب بشكل عام في هذه الفصل، ومفهوم الإرهاب الإلكتروني وذلك من خلال المباحث الآتية:

المبحث الاول: ما هية الإرهاب التقليدي وأسبابه

المبحث الثاني: الفضاء الإلكتروني وعلاقته بالإرهاب والجريمة المعلوماتية

المبحث الثالث: التعريف بالإرهاب الإلكتروني وحرب المعلومات

المبحث الاول

ما هية الإرهاب التقليدي وأسبابه

إن التعريف بأي جريمة ربما يرتبط بشكل أكبر بالتعرف على أسبابها وأساليبها، وربما يكون التعرف على أنواعها سبباً أكبر لتعميق الفهم بها. وتشير الباحثة هنا إلى أنه مهما بذلت محاولات لتعريف الإرهاب فإنها لن تقف على تعريف موحد جامع مانع له، وذلك لاختلاف نظرة المجتمع والنظام العام السائد في كل دولة للإرهاب، لكن قد يكون هناك ثوابت من ناحية قانونية، خاصة ما يتعلق بعنصر الخطر، أو علة ومناط التجريم في الأفعال الإرهابية، كما أننا سنعالج مفهوم الإرهاب سواء التقليدي أم الإرهاب الإلكتروني في هذه الدراسة من وجهة نظر عالمنا الذي نعيش فيه ومن وجهة نظر التشريع الأردني تحديداً.

وتقوم الباحثة في هذا المبحث بالتعرف على مفهوم وبعض أحكام الإرهاب التقليدي، دون الدخول في الجدل الدائر حول المفاهيم، وحول نسبة الإرهاب والجرائم الإرهابية إلى جماعة معينة أو تنظيم معين، وذلك تمهيداً لغزو عالم الإرهاب الإلكتروني، وبحث أحكامه وطرق مكافحته والوقاية منه، والذي تقوم عليه دراستنا أساساً. بالتالي فإن الباحثة تعمل على تقسيم هذا المبحث إلى المطالب الثلاث الآتية:

المطلب الأول: مفهوم الإرهاب بشكل عام وأسبابه

المطلب الثاني: أنواع الإرهاب وأساليبه

المطلب الثالث: طبيعة الإرهاب التقليدي والخطر الناجم عنه

المطلب الأول: مفهوم الإرهاب بشكل عام وأسبابه

تعد كلمة إرهاب ترجمة لكلمة (Terror) الإنجليزية وهي مشتقة من كلمة (Terrere) اللاتينية والتي تعني يفزع أو يرهب، ويوصف كثير من الأشياء بهذا الوصف، فقد تكون لقباً لإمبراطور مثل أن نقول (إيفان الرهيب) أو وصفاً لعصور حكم العنف أثناء الاضطرابات السياسية مثل (حكم الإرهاب أثناء الثورة الفرنسية) أو للتعبير عن حوادث متفرقة يستخدم فيها العنف والتي تعرف باسم الإرهاب الدولي(بولتز وآخرون، 1999، ص13).

وقد أطلق مجمع اللغة العربية في معجمه الوسيط وصف الإرهابيين على الذين يسلكون سبيل العنف لتحقيق أهدافهم (المعجم الوسيط:1، ص376). وتعني كلمة إرهاب حسب واحدة من الاتفاقيات ذات الشأن: الرعب أو الخوف الذي يسببه فرد، أو جماعة، أو تنظيم، لأغراض ليس فقط سياسية، لأن تطور ظاهرة الإرهاب جعلها لا تقتصر على الناحية السياسية فقط، بل اشتملت على النواحي القانونية، والعسكرية، والتاريخية، والاقتصادية، والاجتماعية (الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة، 1998).

وفي ظل الجدل الدولي العميق الدائر حول تعريف الإرهاب ومنذ عشرات السنين، تناولت الباحثة العديد من التعريفات ليس بهدف الوصول إلى تعريف دقيق وواضح ومحدد المعالم ، بقدر الوصول إلى مفهوم يبين ما هية الإرهاب وكنهه، وأشكاله، وأساليبه، والتعرف على صوره، وما يدور حوله من أحكام، ووضعه كجريمة من الجرائم الخطرة. ولذلك تناولت الباحثة ذلك من خلال فرعين: التعريف بالإرهاب (الفرع الأول)، وأسباب الإرهاب بشكل عام في (الفرع الثاني).

الفرع الاول: تعريف الإرهاب

لقد دار تعريف الإرهاب ضمن كثير من المحاولات في السابق مستنداً على عدة محاور فمنهم من حاول تعريفه من خلال معيار اعتباره أسلوب قتال، ومنهم اعتمد معيار الجريمة السياسية، ومن المعايير

الأخرى اعتباره أنه الشيوعية حيناً واليسار حيناً واليمين حيناً آخر ومنهم من أقام التعريف على أنه هو العنصرية أو الإسلام أو الاغتيال السياسي أو قتل الأبرياء أو العنف لأغراض سياسية أو أنه يستند إلى مذهب يتضمن سلوكاً سياسياً غير قانوني ومنهم من اعتبره الحرب أو الأعمال السرية للدولة أو العنف السياسي المنظم (شريف، 1997، ص47-51).

والإرهاب عبارة عن شكل من أشكال العنف المنظم، وقد أصبحت المنظمات الدولية بما فيها الامم المتحدة تستخدم مفهوم اجرائي للعمل الإرهابي، وتتفق على بعض المفاهيم أو الأمثلة للعمل الإرهابي، مثل: الاغتيال، والتعذيب، واختطاف الرهائن (مجلة السياسة الدولية، 1993، ص6).

ومن التعاريف الاصطلاحية للإرهاب من حيث الشمولية وتحديد سلوك الإرهاب، ما توصل إليه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي، الذي عرف الإرهاب بأنه: العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً على الإنسان في دينه، ودمه، وعقله، وماله، وعرضه، ويشمل صنوف التخويف، والأذى، والتهديد، والقتل بغير حق، وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم، أو حريتهم، أو أمنهم، أو أحوالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة، أو المرافق العامة، والأملاك الخاصة، أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها (بيان مكة المكرمة الصادر عن المجمع الفقهي لرابطة العالم الإسلامي، 1422هـ، ص8).

وقد أصدر مجمع الفقه الإسلامي الدولي تعريفاً لمصطلح الإرهاب بأنه:" العدوان أو التخويف أو التهديد مادياً أو معنوياً والصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد(قرار مجمع الفقه الإسلامي الدولي، 1423هـ).

وعلى المستوى العربي قامت لجنة الخبراء العرب المنعقدة في تونس بين 22 و24 آب من العام 1989، بوضع تصور عربي أولي لمفهوم الإرهاب، والإرهاب الدولي لتمييزه عن نضال الشعوب من أجل التحرر، وعرفته أنه:" فعل منظم من أفعال العنف أو التهديد به، يسبب فزعاً أو رعباً من خلال

أعمال القتل، أو الاغتيال، أو حجز الرهائن، أو اختطاف الطائرات، أو تفجير المفرقعات وغيرها، مما يخلق حالة من الرعب والفوضى والاضطراب، والذي يستهدف تحقيق أهداف سياسية، سواء قامت به دولة أو مجموعة من الافراد، ضد دولة أو ضد مجموعة اخرى من الافراد، وذلك في غير حالات الكفاح المسلح الوطني المشروع من أجل التحرير، والوصول إلى حق تقرير المصير، في مواجهة كافة أشكال الهيمنة، أو قوات استعمارية، أو محتلة، أو عنصرية، أو غيرها، وبصفة خاصة حركات التحرير المعترف بها من الأمم المتحدة، ومن المجتمع الدولي، والمنظمات الإقليمية، بحيث تنحصر أعمالها في الأهداف العسكرية أو الاقتصادية للمستعمر، أو المحتل أو العدو، ولا تكون مخالفة لمبادئ حقوق الانسان، وأن يكون نضال الحركات التحررية وفقاً لأغراض ومبادئ ميثاق الأمم المتحدة، وسواه من قرارات أجهزتها ذات الصلة بالموضوع" (التل، 1998، ص13).

كما وضع وزراء الداخلية والعدل العرب في الاتفاقية العربية لمكافحة الإرهاب، الصادرة في القاهرة عام 1998م تعريفاً له بأنه:" كل فعل من أفعال العنف أو التهديد، أياً كانت بواعثه وأغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بأحد المرافق، أو الأملاك العامة أو الخاصة، أو اختلاسها، أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر(الاتفاقية العربية لمكافحة الإرهاب، 1998).

وعرفه مكتب المباحث الفيدرالية الأمريكي (اف بي آي) أنه:" استخدام غير مشروع للقوة، ضد الأشخاص أو الممتلكات، ليسيء إلى الحكومة، أو المدنيين، أو قطاع من المجتمع، وذلك لتحقيق أهداف سياسية أو اجتماعية (شكور، 1997، ص31، من: علوان، 2008، ص18).

وعلى المستوى الدولي تم تعريف الإرهاب في أكثر من مناسبة وأكثر من طريقه، فقد عرفته الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م بأنه:"الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها، أو من شأنها إثارة الفزع أو الرعب، لدى شخصيات معينة، أو جماعات من الناس، أو لدى العامة"(موقع سوريا الحرة، وثائق وحقائق الإرهاب الدولي، 2004).

كما عرف الإرهاب في المادة الأولى من اتفاقية جنيف الأولى الخاصة بمكافحة الإرهاب الدولي أنه: "الأفعال الإجرامية الموجهة ضد الدولة والتي يتمثل غرضها أو طبيعتها في إشاعة الرعب لدى شخصيات معينة أو مجموعات من الأشخاص أو لعامة الشعب".

وعرف الإرهاب الداخلي أنه الذي يقدم عليه الجاني بإرادته المنفردة أو ذلك الإرهاب الذي ينفذ دون خطة مرسومة من قبل دولة ضد دولة أخرى، وهو الإرهاب الذي عنته المادة 147 من قانون العقوبات الأردني، التي سنأتي عليها لاحقاً.

وفقهياً فقد عرف الإرهاب أنه:" استراتيجية عنف محرم دولياً، تحفزها بواعث عقائدية (آيديولوجية)، وتتوخى إحداث رعب داخل شريحة خاصة من مجتمع معين، لتحقيق الوصول إلى السلطة، بغض النظر عما إذا كان مقترفو العنف يعملون من أجل أنفسهم ونيابة عنها، أم نيابة عن دولة من الدول" (Bassioni. 1983،P. 22 ، من: علوان، 2008، ص18).

كما عرف أنه:" استخدام متعمد للعنف أو التهديد، باستخدام العنف من قبل بعض الدول، أو من قبل جماعات، تشجعها وتساندها دول معينة، لتحقيق أهداف سياسية واستراتيجية، وذلك من خلال ممارسة أفعال خارجة على القانون، تستهدف خلق حالة من الذعر الشامل في المجتمع" (اسماعيل، 1996، ص144).

أما الفقه الغربي فمنهم من عرفه أنه:" نوع من العنف المتعمد تدفعه دوافع سياسية، موجه نحو أهداف معينة، تمارسه جماعات معينة، أو عملاء سريون لإحدى الدول (مورجان . ك، الإرهاب والعنف، مترجم عن الانكليزية، الدار العربية للكتاب، القاهرة، 1989، ص 14، من: علوان، 2008، ص17).

ومنهم من عرفه أنه:" القتل العمد المنظم الذي يهدد الأبرياء، ويلحق الأذى بهم، بهدف خلق حالة من الذعر، من شأنها أن تعمل على تحقيق غايات معينة" (كوفال . م، 2008، ص17).

ومن التعريفات أيضاً تعريف (غوشيه) أنه: "أشكال القتال قليلة الأهمية بالنسبة للأشكال المعتمدة في النزاعات التقليدية. ألا وهي قتل السياسيين أو الاعتداء على الممتلكات". كما عرف أنه: "الاستعمال العمدي والمنظم لوسائل من طبيعتها إثارة الرعب بقصد تحقيق الأهداف". كما عرفه (جوليان فرويند) أنه:

"استعمال العنف دون تقدير أو تمييز بهدف تحطيم كل مقاومة وذلك بإنزال الرعب في النفوس. وأنه فعل سيكولوجي لا يرمي فقط كما في فعل العنف إلى القضاء على أجساد الكائنات وتدمير الممتلكات المادية، بل يستعمل العنف بشكل منسق ليخفيف النفوس ويرهقها (هذه التعريفات من: الفتلاوي، 2005، ص98).

وبالرغم من التعاريف التي تناولت الإرهاب التقليدي، إلا أنها بمجملها تبقى قاصرة، لأنها قد تختلط مع بعض الأفعال التي تعد من باب الحقوق، كالحق بالمقاومة، وتقرير المصير، وحق الشعوب في الدفاع عن أوطانها ومستقبلها ومصيرها.

ويمكن تعرف الارهاب انه تعمد العنف أو التهديد به من قبل بعض الدول والجماعات لتحقيق أهداف سياسية بأفعال غير قانونية ومن خلال خلق حالة من الذعر وقتل عمد ومنظم للأبرياء او الحاق الضرر والأذى بهم.

وتختلف المقاومة عن الإرهاب، فللمقاومين الذين احتلت بلادهم الحق في المقاومة والدفاع عن أوطانهم (شلالا، 2003، ص18). وقد أقرت اتفاقية لاهاي الرابعة لسنة 1907 بأن هبة شعب إقليم ما للدفاع الوطني ضد الغزاة يجعلهم كالمحاربين إذا كانوا يحملون السلاح علناً واحترموا القواعد القانونية للحرب.

كما يسيطر أحياناً على التعريف، تلك المفاهيم التي تقدمها بعض الدول المسيطرة في العالم، كالولايات المتحدة الامريكية، التي تعرف الإرهاب أنه:" كل عمل يتعارض مع المصالح الامريكية هو عمل إرهابي، سواء كان تفجيرياً أم نظرياً". ونتيجة للنظرة الامريكية للإرهاب فقد ظهر مفهوم الإرهاب الإلكتروني (النابلسي، 2011، بدون رقم صفحة).

وتشريعياً نجد أن قانون العقوبات الأردني قد عرف الإرهاب أنه:" استخدام العنف بأي وسيلة كانت، أو التهديد باستخدامه، أياً كانت بواعثه وأغراضه، يقع تنفيذاً لمشروع اجرامي فردي أو جماعي، يهدف إلى تعريض سلامة المجتمع وأمنه للخطر، إذا كان من شأن ذلك إلقاء الرعب بين الناس وترويعهم، أو تعريض حياتهم للخطر، أو الحاق الضرر بالبيئة، أو المرافق والأملاك العامة أو الأملاك الخاصة، أو المرافق الدولية، أو البعثات الدبلوماسية، أو باحتلال أي منها، أو الاستيلاء عليها، أو تعريض الموارد

الوطنية للخطر، أو ارغام أي حكومة أو أي منظمة دولية أو إقليمية، على القيام بأي عمل أو الامتناع عنه" . ويعد من جرائم الإرهاب الأعمال المصرفية المشبوهة، المتعلقة بايداع الأموال أو بتحويلها إلى أي جهة لها علاقة بنشاط إرهابي (المادة 147 من قانون العقوبات الأردني)[3].

وترى الباحثة أن هذا النص يتسم بالتقليدية نوعاً، ما ولا يتسم بالشمول الذي يظهر من خلال الأهداف المستهدفة في العمليات الإرهابية، ويخلو من التطرق إلى الفضاء الإلكتروني كوسيلة اتصال سواء كطريقة من طرق تنفيذ وتسهيل العمليات الإرهابية أم كانت هدفاً لتلك العمليات الإرهابية.

وهناك تعريف موسع في قانون العقوبات الإسباني، قد يكون أوسع وأشمل، حيث نصت المادة 260 منه على أن: "يعتبر من قبيل الأعمال الإرهابية كل فعل يتوخى الاعتداء على أمن الدولة الداخلي أو النظام العام أو السلامة الاجتماعية، فيرمي إلى تخريب وتعطيل الأشغال العامة، والمصانع، والأبنية العسكرية، والكنائس، والأماكن الدينية، والمتاحف، والمكتبات، والمخطوطات، وممتلكات الدولة والأفراد، والجسور، والسدود، والمرافئ، والقنوات، وسبل النقل والمواصلات، والاتصالات، وخطوط الشبكات الكهربائية والهاتفية، والمناجم، ومصانع البارود، ومستودعات المحروقات على كافة أنواعها، والبواخر، والطائرات، والكوارث الطبيعية التي تنشأ عن ذلك، ولاسيما الإحراق، والإغراق، والتسبب بالقتل، وذلك نظراً للمواد المتفجرة والخانقة، وغير ذلك من المواد الفتاكة بالإنسان"(شلالا، 2003، ص18).

وأخيراً تجدر الإشارة إلى تمييز الإرهاب الداخلي عن الإرهاب الدولي، حيث أنهما يختلفان عن بعضهما من حيث موضوعهما، أي ضمن معيار موضوعي، والذي ينحصر في موضوع الجريمة أو الغرض الذي يبتغيه الجاني، فإذا انصب على النظام الاجتماعي أو السياسي الداخلي كان الإرهاب داخلياً، وإذا امتد الموضوع إلى العلاقات الدولية يكون الإرهاب دولياً. كما قد يكون الإرهاب داخلياً متى كان

---

3 هذه المادة معدلة بالقانون رقم 16 لسنة 2007، حيث كان نصها السابق كما يلي:"يقصد بالأعمال الارهابية جميع الأفعال التي ترمي إلى ايجاد حالة ذعر وترتكب بوسائل كالأدوات المتفجرة، والمواد الملتهبة، والمنتجات السامة أو المحرقة، والعوامل الوبائية، أو الجرثومية التي من شأنها أن تحدث خطراً عاماً".

الغرض منه الحصول على مغنم مادي أو فرض مذهب سياسي أو العمل على تغيير شكل الدولة(عبيد، 1979، ص225. ومحب الدين، د.س، ص212).

الفرع الثاني: أسباب الإرهاب بشكل عام

بالرغم من وجود تفاوت في المفاهيم بين الإرهاب الدولي والإرهاب العادي، إلا أنهما يتماثلان إلى حدود بالغة، من حيث الأفعال والأهداف، وفي صدد الحديث عن الإرهاب الدولي، هناك لجنة تابعة للأمم المتحدة خاصة بالإرهاب الدولي، وقد حددت هذه اللجنة أسباب الإرهاب في تقريرها المؤرخ بتاريخ 29 فبراير 1979 كالآتي (التل، 1998، ص19-20):

أولاً: الأسباب السياسية: ومنها سيطرة الدول على بعضها البعض في حالات كالاستعمار، والتمييز العنصري، واستخدام القوة ضد الدول الضعيفة، والتدخل في الشؤون الداخلية للدول الأخرى، والاحتلال الأجنبي الكلي أو الجزئي، وممارسة القمع والعنف للتهجير أو للسيطرة على شعب معين.

ثانياً: الأسباب الاقتصادية: ومنها عدم التوازن في النظام الاقتصادي العالمي، والاستغلال الأجنبي للموارد الطبيعية للدول النامية.

ثالثاً: الأسباب الاجتماعية: ومنها انتكاك حقوق الإنسان بالتعذيب أو السجن أو الانتقال، والجوع والحرمان والبؤس والجهل، وتجاهل معاناة الشعوب التي تتعرض للاضطهاد، وتدمير البيئة.

ومن الأسباب أيضاً، المؤثرات الخاصة، والتي ترتبط بالأسباب السابقة، وهو ما يعرف بالمؤثرات الخاصة بحدوث الإرهاب، ومن هذه المؤثرات: طبيعة الأرض التي تساعد الإرهابيين في الاختفاء وارتكاب جريمتهم، إلى جانب المناخ السائد، وطبيعته ومدى توافر المواد الغذائية، والاكتفاء الذاتي لدى التنظيمات أو الجماعات، وأحياناً قد يكون للخمور والإدمان دور في هذه المسألة، ومن المؤثرات أيضاً نقص الألفة بين الأجناس وعدم اندماج أبناء جنس معين بجنس آخر، فتلجأ بعض الدول إلى التشجيع على الزواج المختلط لذلك. ووجود المركزية الإدارية خاصة في الدول التي تجاوزت مرحلة النمو، فتصبح

مسألة عدم وجود اللامركزية من المؤثرات الخاصة بحدوث الإرهاب. وكذلك عدم وجود نقابات قوية لعدم وجود جهة تستجيب لأماني العمال والطوائف الأخرى. وكذلك عدم السماح للاجتماعات العامة لالتقاء الناس ببعضها، وعدم إشراك بعض الطوائف بالتمثيل، وعدم مراعاة السن المطلوب لإشراك أكبر شريحة، ولإشراك الشباب في العملية السياسية، لتجنب إشعارهم بالفراغ السياسي مما يدفعهم إلى الانحراف على طريق الإرهاب. وكذلك عدم إعادة النظر في أنظمة القضاء والدفاع من حين لآخر، للتأكد من رضى الرأي العام عن مسار القضاء في البلاد. وعدم اللجوء إلى الاستفتاء الشعبي أو الاستفتاء السياسي الذي يتضمن إشراك الشعب في الحياة السياسية من خلال أخذ رأيه في المسائل الهامة (صدقي، 1985، ص100-103).

ومن الأسباب أيضاً الفراغ الفكري، حيث يؤثر الفراغ الفكري بالمسألة الأمنية، أو الأمن الفكري، بالتالي فان تحقيق الأمن لا بد وأن يكون أمناً شاملاً من بينها تحقيق الأمن الفكري، وقبل التطرق لمفهوم الأمن الفكري، لابد من الإشارة إلى أن أهم أسباب اختلال الأمن الفكري هو الفراغ الفكري لدى البعض، ويؤثر الفراغ الفكري في ذلك من خلال عوامل تتمثل بـــ: عدم القدرة على المشاركة في صنع القرارات، وعدم القدرة على حل المشاكل التي قد تواجهها، وشعور الإنسان بأنه ليس له أهمية، والفشل في الحياة العلمية والاجتماعية وغيرها من الجوانب الحياتية(نظمي، 2010، ص12).

ويحتل مفهوم الأمن الفكري أهمية بالغة، إذ أنه يحقق الأمن والاستقرار في المجتمع، من خلال التصدي للمؤثرات والانحرافات الفكرية. وقد لاقت مسألة الأمن الفكري أهمية على مر الأزمنة والعصور، وزادت أهميتها في الآونة الاخيرة في ظل الحروب والغزوات الفكرية. حيث أن الغزو الفكري يعد من المفاهيم الحديثة، ويعني مجموعة الجهود التي تقوم بها أمة من الأمم للاستيلاء على أمة أخرى، أو التأثير عليها حتى تتجه وجهة معينة. ويعد الغزو الفكري ذا خطر أكبر من الغزو العسكري، لأنه يقوم على السرية وسلوك المسارب الخفية، مما يؤدي إلى عدم احساس الأمة المغزّوة به، وعدم امكانية صده والوقوف في وجهه فتقع ضحاياه فريسة له وتصبح مريضة الفكر والإحساس.

ويحتل الأمن الفكري -كعنصر من عناصر المنظومة الأمنية- أهمية بالغة، حيث سبق وأن أشارت الباحثة أنه يعني الحفاظ على المكونات الثقافية الأصلية في مواجهة التيارات الثقافية الوافدة أو

الأجنبية المشبوهة، بالتالي فإنه يهدف إلى حماية الهوية الثقافية من الاختراق أو الاحتواء من الخارج، ويعمل على الحفاظ على العقل من الاحتواء الخارجي، خاصة في ظل ما يتميز به هذا العصر من مزايا وتطورات تقنية وتكنولوجية ساعدت على التقارب بين المجتمعات والشعوب، وانفتاحها على بعض، واختلاط الثقافات وتبادلها، وتأثرها ببعضها البعض، ودخول التيارات الفكرية الوافدة إلى ثقافات الشعوب، بايجابياتها وسلبياتها، وهذا ما اثر على الثقافات والافكار، ودفع باتجاه الأمن الفكري وتكريسه، لأن الانحراف الفكري أصبح من أهم أسباب ودوافع الإرهاب (نظمي، 2010، ص13).

وترى الباحثة أن أهمية هذا النوع من الغزو تزداد في ظل التطورات التقنية الحديثة والتطور التكنولوجي في مجال الاتصالات والانترنت، حيث قلل الانترنت المسافات بين الناس، وأدى إلى اندماج الثقافات ببعض، الأمر الذي سهل من عملية الغزو الفكري، وبالتالي استخدام تلك القيم الجديدة في العمليات الإرهابية، أهدافاً أم وسائلاً.

ومع ذلك ليس المقصود بتكريس وتحقيق الأمن الفكري للأمة، أن نقطع العلاقات مع الثقافة العالمية، ونتهمها بغزو العقول، لأن الانسان بطبعه يحتاج ثقافات الشعوب الأخرى ليأخذ منها ما يتوافق وقيمه، وعقائده، وثوابته، ومبادئه، وأخلاقه، والعمل على نشر ثقافته بين الآخرين.

بالتالي يمكن القول أن من أسباب الإرهاب أيضاً، تلك التطورات العلمية والتكنولوجية، حيث بدأ ذلك مع الثورة الصناعية في أوروبا والولايات المتحدة، ثم اكتشاف الطاقة الذرية وأسرارها، والتطورات الهائلة في مجالات الفضاء، والمعلومات، والعقول الإلكترونية، والتطورات الهائلة في مجال الاتصال والنقل، وإيجاد العديد من الأهداف الحساسة التي أثرت بشكل رئيسي في الحضارة المعاصرة.

ومن آخر التطورات وأهمها، ثورة الحاسوب والاتصالات والإنترنت، وما سببته من تطورات في مختلف المجالات. وقد أدت كل تلك التطورات إلى خلق نوع من التطور في جهة، يقابله نوع من التخلف الحضاري لدى جهات أخرى، جعلها تذهب باتجاه إنشاء تنظيمات وحركات تحرر ضد الدول الاستعمارية المتطورة. كما قد دفعت تلك التطورات إلى الانتقام والتنظيم لمقاومة هذه الحالة من التطور (الفتلاوي، 2005، ص113-114).

وبالذهاب إلى الإرهاب المعلوماتي، تجد الباحثة أن الأسباب السابقة تنطبق في حالة الإرهاب الإلكتروني، إذ نجد أن الأسباب السياسية يمكن ملاحظتها عن طريق الإنترنت، وممارسة العمل السياسي أو الحرمان منه قد يظهر من خلال الإنترنت، مما يجعل الإنترنت سبب من الأسباب السياسية، وأحياناً من الأسباب الاقتصادية، وأحياناً من الأسباب الاجتماعية. وسيتم البحث بشكل تفصيلي لاحقاً عن أسباب الإرهاب الإلكتروني.

المطلب الثاني: أنواع الإرهاب وأساليبه

إن الحديث عن أنواع الإرهاب وأشكاله وأساليبه يتشابه مع الحديث عن الإرهاب من حيث تعريفه، فمثلما تتعدد التعريفات التي تناولت الإرهاب، والتي عرفته من عدة زوايا، فإن التقسيمات التي بحثت في أنواع الإرهاب أيضاً قد تعددت تبعاً لها، وحسب الزاوية التي ينظر منها إلى الإرهاب، بالتالي نتناول في هذا المطلب الحديث عن هذه الانواع حسب الأهمية، والبحث في أشكال الإرهاب التي قد تكون زاوية ينظر منها لتقسيمه، وكذلك الحال بالنسبة لأسبابه.

الفرع الأول: أنواع الإرهاب بشكل عام

يرى جانب من الفقه أن للإرهاب ثلاثة أنواع:

أ. الإرهاب ضد النظام القائم للإطاحة به، وينتهي بقيام نظام بديل، أو بانتصار النظام القائم على معارضيه. وهذا قد يتشابه مع الثورة أحياناً إلا أنه يتميز من حيث الغايات والوسائل المتبعة في ذلك(التل، 1998، ص31).

ب. إرهاب الدولة، وهو الذي يتم بعد الوصول إلى السطة، فتقوم المجموعة التي وصلت السلطة، لتصفية آثار العهد والنظام السابق وتدمير مرتكزاته(السماك، 1992، ص62).

ج. الإرهاب الذي تمارسه منظمات التحرير الوطنية: إذ أنه وعند عجز هذه المنظمات عن شن حرب واسعة النطاق تلجأ إلى القيام بالعمليات الإرهابية(التل، 1998، ص32).

ولا تتفق الباحثة مع هذا التقسيم، فبداية قد يكون هناك إرهاب دولة، إلا أنه ليس بالمعنى الذي يتم من خلال الجماعة التي تصل إلى السلطة، لأنها قد تكون جماعات ناضلت لتحقيق الحرية والتخلص من الظلم والاستبداد. إلا أن إرهاب الدولة برأي الباحثة ذلك الذي يتم من خلال استبداد وتسلط بعض الدول المسيطرة والمهيمنة على الدول الأخرى، وخاصة ما يتم من خلال الاحتلال، وأبرز أمثلته ما نعيشه في عالمنا الحاضر من إرهاب دولة الكيان الصهيوني بحق الشعب الفلسطيني الحر الأبي.

وقد يكون هناك إرهاب ضد نظام قائم فيما إذا كان نظاماً عادلاً، وهناك من يعارض على أسس غير سليمة، ترتبط بالتمييز العنصري والديني والعقائدي، فتتشكل بعض الجماعات للإطاحة بالنظام بهدف السيطرة والتخريب على النظام القائم، طمعاً بالسلطة فتقوم بتنفيذ العمليات والهجمات الإرهابية تحقيقاً لغاياتها.

أما إرهاب منظمات التحرير فإنه تقسيم يجافي الواقع والمنطق، إذ أن المعنى البديهي للتحرير يرتبط بحق الشعوب بتقرير مصيرها، وهو أهم حق من الحقوق الجماعية للإنسان، وهناك كثير من الشعوب تعاني من الظلم والبطش والاستبداد والقمع والاحتلال، فتلجأ للتعبير عن حقها بتقرير مصيرها بالوسائل السلمية، إلا أنها تتعرض للقمع والسجن والتعذيب، مما يبدأ معه البعض بتشكيل جماعات تسمى حركات التحرير أو منظمات التحرير، التي تناضل في سبيل الحرية، بالتالي لا يمكن القول بأن ذلك يمثل نوعاً من الإرهاب.

وهذا التقسيم حسب ما تلاحظ الباحثة يستند إلى الطريقة أو الجهات التي تنفذ الهجمات الإرهابية. إلا أن هناك تقسيم آخر وهو ما استندت إليه دراستنا ابتداء، وهو التقسيم من حيث الطريقة التي يتم من خلالها تنفيذ العمليات الإرهابية، وهنا يمكن القول بوجود نوعين من الإرهاب:

أ. الإرهاب التقليدي: وهو المعروف باستخدام الوسائل التقليدية، وينفذ هجماته في بيئة تقليدية أيضاً.

ب. الإرهاب الإلكتروني: وهو ما يتم بوسيلة إلكترونية، أو يتم اعتداء على بيئـــة إلكترونيـــة، أو أن تساهم البيئة الإلكترونية في تنفيذ هجماته.

وهذا النوع الأخير هو ما تقوم عليه دراستنا التي تتناول الإرهاب الإلكتروني كواحداً من أهم صـــور الإرهاب في الوقت الحالي. والذي ينطوي تحته كافة صور الإرهاب التقليدي، فقد يكون هنـــاك إرهـــاب دولة بوسائل إلكترونية، وقد يستهدف إرهاب الدولة بيئة إلكترونية، وقد تستخدم الجماعات الإرهابية البيئة أو الفضاء الإلكتروني لتنفيذ هجماتها، أو أن هجماتها قد تستهدف بيئة إلكترونية. وكلا النوعين قد يستخدم الفضاء الإلكتروني لتسهيل عملياته وإخفائها والتخطيط والتدريب لها.

وتأكيداً على ما سبق نخلص إلى نوعين من الإرهاب من حيث مرتكب الجريمة وهما:

1- **إرهاب الدولة:** ويتم من خلال دولة، ضد دولة أو جماعات أو أفراد. **ومـــن أســـاليب الإرهـــاب الدولي:** اختطاف الطائرات: بسبب كلفة الطائرات وإثارة عمليات الخطف للإعلام الدولي وغالباً ما تنقل الطائرات أشخاص مهمين ورسميين وعادة ما تحمل عدد كبير مـــن الأشـــخاص ومـــن جنسيات مختلفة. واختطاف الأفراد: غالباً ما يكونوا من المتمتعين بمراكز سياسية معينة لمساومة دولهم للحصول على بعض المطالب. واختطاف دبلوماسيين. وضرب مقار السفارات الأجنبيـــة. وتفجير القنابل في المحلات العامة. نشر الأمراض الوبائية كالجمرة الخبيثة (للتعمق: العـــازمي، 2007، ص41-46).

2- **إرهاب المنظمة أو الجماعة:** ويتم من خلال تنظيم ضد تنظيم آخـــر، أو ضـــد دولـــة، أو ضـــد مجموعة من الأفراد(العازمي، 2007، ص46).

الفرع الثاني: أساليب الإرهاب وأشكاله

تتخذ العمليات الإرهابية بشكل عام خاصة في ظل الإرهاب التقليدي بنوعيه، إرهاب الدولـــة أو إرهاب التنظيم، بعض الصور والأشكال من الجرائم التي تتمثل بـــ:

أولاً: حرب العصابات، ومثالها تلك الحرب التي دارت في أمريكا اللاتينية، بعد نجاح الثورة الكوبية عام 1959، في كولومبيا وبوليفيا وغواتيمالا وفنزويلا والبرازيل، والتي كان رائدها (تـــشي غيفـــارا)، وقـــد واجهتها الولايات المتحدة الأمريكية بتنظيمات مسلحة مولتها ودربتها، مثل: منظمة (ماكوتشي) ومنظمـــة (تونتسي) في هاييتي و(فرقة الموت) في البرازيل(التل، 1998، ص34).

وتختلف أهداف العصابات التي تشن الهجمات الإرهابية تبعاً لاختلاف الأسباب والـــدوافع لإنـــشائها وتنظيمها، فقد تكون لمواجهة نظام قائم، أو قد تكون لإثارة الرعب والذعر بين الناس، وقد تكون لأسباب اقتصادية أو للحصول على المال، أو قد تكون لأسباب طائفية أو عرقية أو دينية.

ثانياً: الاغتيالات السياسية، أي التصفية الجسدية لأشخاص معينين تستهدف الجهة القائمة على تنفيذ العملية الإرهابية، ومثال ذلك اغتيال الشيخ أحمد ياسين، وعبدالعزيز الرنتيسي زعماء حركة حماس، علـــى يـــد الاحتلال الإسرائيلي. ومن الأمثلة القديمة اغتيال ولي عهد النمسا وزوجته في مدينة ســـراييفو احتجاجـــاً على ضم البوسنة والهرسك إلى الإمبراطورية النمساوية المجرية، والتي كانت من أسباب اشتعال الحرب العالمية الأولى(العازمي، 2007، ص58-59).

ثالثاً: احتجاز الرهائن، أي التوقيف والاحتجاز القسري لشخص أو أشخاص ليسوا أطرافاً مباشرين فـــي نزاع، يقصد المحتجزون أو المختطفون بواسطتها فرض شروطهم السياسية، أو العـــسكرية، أو الماليـــة، على الذين هم في نزاع معهم. وتتم العملية للمساومة عليهم، وخلق نوع مـــن الخطـــر لتـــدعيم مـــوقفهم

التفاوضي مع الطرف الآخر (السماك، 1992، ص40). وقد لا يستهدف الخاطفون قتل الرهائن. ومن الأمثلة الحديثة أزمة الرهائن في المدرسة الروسية[4]، حيث أفضى الأمر إلى قتل بعض الرهائن.

وتبرز ظاهرة احتجاز الرهائن بشكل أكبر في الغايات الاقتصادية من وراء العمليات الإرهابية، فقد تتم للضغط على ذوي شخص لدفع مبالغ طائلة من الأموال للإفراج عن الرهائن. وقد تتم لأسباب عسكرية غير إرهابية أثناء مقاومة المحتل، كما قامت حركة حماس باستبدال ما يقارب الألف أسير فلسطيني مقابل جندي اسرائيلي تم اختطافه في غزة(شاليط)، إلا أنه لا يمكن القول أن عملية الخطف هذه عملية إرهابية، إلا إذا كانت تستهدف الأبرياء المدنيين العزل، لتحقيق أهداف سياسية تتعارض مع حقوق الإنسان، وإقامة العدل والنظام في المجتمع.

رابعاً: خطف الطائرات، أي الاستيلاء على طائرة أثناء تحليقها في الجو، عن طريق اللجوء إلى التهديد المقنع باستخدام العنف، وإجبار طاقمها على تغيير وجهة سيرها، والتوجه نحو مطار آخر محايد أو صديق للمختطفين، وذلك لعقد صفقة والحصول على تنازلات مقابل الإفراج عن المختطفين والطائرة. وهناك الكثير من الأمثلة لهذه العمليات وقعت في العقود الماضية (العازمي، 2007، ص52-53).

خامساً: ضرب المدنيين بالقنابل، الأصل في هذه الأعمال أنها محرمة -حتى في حالة الحرب- إذ لا يجوز ضرب المدنيين واستهدافهم، وذلك كقاعدة مستقرة في القانون الدولي الإنساني وقانونم الحرب. إذ أن هناك اتفاقية كاملة لحماية المدنيين من بين اتفاقيات جنيف الأربع، وهي الاتفاقية الرابعة التي تتعلق

4 تتلخص وقائع هذه الأزمة أو ما يعرف بأزمة رهائن مدرسة بسلان أو مجزرة بسلان، وهي عملية اقتحام مجموعة مسلحة مدرسة ببلدة بيسلان في روسيا، حيث عملت على احتجاز أكثر من 1100 رهينة، بتاريخ 2004/12/1، وبعد ثلاثة أيام من الحصار اقتحمت القوات الروسية المدرسة بالدبابات والأسلحة الثقيلة، حيث أسفر ذلك عن مقتل حوالي 320 رهينة، بينهم 186 طفل، وأصابة الأخرين (ويكيبيديا الموسوعة الحرة على الانترنت: http://ar.wikipedia.org.

بحماية المدنيين أثناء النزاعات المسلحة. وذلك إلى جانب تحريم باقي اتفاقيات جنيف لاستهداف المدنيين، كما أن هناك الكثير من المواثيق الدولية التي تحرم استهدافهم، حتى بات ذلك من القواعد الآمرة في القانون الدولي.

وكذلك الحال في غير أوقات النزاعات المسلحة، فاستهداف المدنيين أثناء النزاعات المسلحة يعد جريمة حرب، وفي غير أوقات النزاعات المسلحة أيضاً، وتعد هذه الأعمال إذا ما ارتكبت في غير أوقات النزاعات المسلحة جرائم ضد الإنسانية أو جرائم إبادة جماعية. لذا فإن استهداف المدن وضربها بالقنابل يعد وسيلة حربية وهذا هو الإرهاب بأم عينه.

سادساً: احتجاز السفن، سواء في المياه الإقليمية لدولة ما، أو في أعالي البحار، وتسمى الجريمة الثانية القرصنة في أعالي البحار. وتتم لإرغام الدولة صاحبة السفينة لإجابة طلبات الجهة المحتجزة، أو إطلاق التعهدات لإجابة هذه الطلبات.

سابعاً: الاستعمار الاستيطاني، ويعد من أهم وأخطر صور الإرهاب، ويتمثل بوجود أشخاص مزروعين وسط محيط من سكان البلاد الأصليين، يشعرون بالنقاء والتفوق العرقي، يمارسون إزاء السكان مختلف أنواع التمييز العنصري، وينكرون عليهم وجودهم القومي(التل، 1998، ص42). ومثال ذلك احتلال اليهود للاراضي الفلسطينية، وما يمارسونه بحق الشعب الفلسطيني من جرائم واعتداءات وانتهاكات لحقوقهم.

ثامناً: احتلال الأراضي والتوسعة الإقليمية، ويتشابه ذلك مع الاستعمار والاحتلال ويعد التوسع الإقليمي من صور الاحتلال.

وأخيراً، بالرجوع إلى موضوع دراستنا –الفضاء الإلكتروني– كوسيلة أو هدف للعمليات الإرهابية، وربط ذلك بأشكال الإرهاب المختلفة وأساليبه، وتتبع هذه الأشكال واحدة تلو الأخرى، نجد أن الإنترنت أو الفضاء الإلكتروني يمكن أن يكون وسيلة للقيام بكافة هذه الصور، بما في ذلك الاغتيال والاستعمار. كما قد يكون الإنترنت ذاته هدفاً للعمليات الإرهابية، لتدمير بنية المعلومات لدى جهة معينة.

وتتفاوت التعريفات المتعلقة بالإرهاب بتفاوت النظرة إليه أو إلى الأعمال أو الأفعال المكونة له فبعض الأفعال قد تعد مشروعة من وجهة نظر مرتكبها ولا تكون كذلك من وجهة النظر الأخرى وهذا ما تسبب بظهور مفاهيم جديدة للإرهاب في العالم المعاصر. كما أن النظرة الغربية تختلف عن النظرة الشرقية للإرهاب، ومع ذلك هناك كثير من الأفعال لا يختلف عليها اثنان من حيث اعتبارها أعمالاً إرهابية وإن اتخذت صوراً أو تسميات أخرى أو لجرائم أخرى كما هو الحال في جرائم الحرب والجرائم ضد الإنسانية وجرائم الإبادة الجماعية والعدوان.

أما بالنسبة لأشكال الإرهاب، فيرى البعض أن أشكال الإرهاب كالتالي(فتلاوي، ص106-109):

أ. **الإرهاب الثوري:** الذي يرتكب من قبل تنظيمات لها القدرة على استلام السلطة أو إجراء التغيير في الأنظمة القائمة فتقوم بعمليات ضد مؤسسات الدولة لتحقيق غاياتها.

ب. **الإرهاب الفوضوي:** توجيه أعمال انتقامية ضد السلطة لعدم تطبيقها العدالة، وتضييقها من الحريات.

ج. **الإرهاب المضاد:** من الأفراد أو الجماعات ضد السلطة أو من السلطة ضدهم لتخوينهم مثل منظمة المستعربون والدوبريان وأمان الصهيونية التي تمارس أعمالاً إرهابية ضد الشعب الفسطيني.

د. **الإرهاب المميز:** الذي يستهدف أهداف أو أشخاص محددين مسبقاً بالنظر لأهميتهم.

ه. **الإرهاب الأعمى:** وهو العشوائي الموجه نحو المدنيين والأهداف المدنية.

و. **الإرهاب السياحي:** الذي يستهدف السياح.

ز. **الإرهاب الصادر عن منظمات حكومية:** أي تشكيل قوات من غير الجيش والأمن في بعض الدول لتحقيق أهداف النظام والتغلغل في صفوف المعارضة.

ح. **إرهاب الأقلية:** وهو ما تمارسه الأقليات للضغط باتجاه الحصول على استقلالها والمطالبة بالحكم الذاتي والمطالبة ببعض الحقوق الخاصة بها.

ط. **الإرهاب بالوسائل العلمية:** حيث لجأت الكثير من التنظيمات الإرهابية إلى استخدام الوسائل العلمية في تنفيذ عملياتها، ومن ذلك الجمرة الخبيثة التي أرسلت عبر البريد لبعض الموظفين من الجهات الحكومية، ومنها وضع مادة مسببة للعقم في مياه المدارس للطالبات الفلسطينيات في عهد الإرهابي "مناحيم بيغن".

المطلب الثالث: طبيعة الإرهاب االتقليدي والخطر الناجم عنه

استكمالاً لحلقات التعرف على ما هية الإرهاب التقليدي، تمهيداً للتعرف على الإرهاب الإلكتروني، وبيان ما هيته وأحكامه، ودراسة حيثياته وأسبابه ووسائله وأنواعه، والوضع القانوني والتجريمي له في قانون العقوبات الأردني، وطرق مكافحته والوقاية منه. فإنه لابد من التعرف على طبيعة الإرهاب بشكل عام، لأن الإرهاب هو الإرهاب، ولكن ما يميز الإرهاب الإلكتروني –كما سنرى– هو الطريقة التي يتم بها ارتكاب الجريمة، وأحياناً محل التجريم. بالتالي فإن طبيعة الإرهاب في النوعين واحدة تستند إلى استخدام عنصر الترويع والتخويف لتحقيق أهداف معينة، من خلال القيام بأفعال قد تكون مجرمة بذاتها أو بمجموعها.

ويمكن التعرف على طبيعة الإرهاب من خلال بيان أهدافه والتعرف عليها، وتتعدد هذه الأهداف كما سنرى، إلا أنها تساعد على فهم أسباب الإرهاب وغايات الإرهابيين والعوامل التي تؤثر به. من هنا تقوم الباحثة بتناول هذا المطلب من خلال تقسيمه إلى فرعين:

الفرع الأول: أهداف الإرهاب وطبيعته

الفرع الثاني: خطر الإرهاب

الفرع الاول: أهداف الإرهاب وطبيعته

ترى الباحثة ضرورة التعرف على أهداف الإرهاب بشكل عام، للتعرف على طبيعته، ومن خلال البحث يمكن التعرف على عدد من الأهداف التي تسعى الجماعات الإرهابية إلى تحقيقها وهي(الفتلاوي، 2005، ص110–116):

أ. الإعلان والتمهيد لظهور الحركة: حيث قد تعلن بعض الحركات عن نشأتها من خلال تنفيذ أعمال وهجمات إرهابية تعبيراً عن ولادتها وتذكيراً بأنها موجودة ولها نشاطاتها وقدراتها.

ب. التعبئة لتأييد الحركة وكسب تأييد الجماهير خاصة عند تبني مطالب جماهيرية وشعبية.

ج. التخلص من العناصر المعادية: كالرغبة بالتخلص من بعض المعادين لقضية وأهـداف الحركـة لإضعافهم والتأثير عليهم.

د. أهداف سياسية: بسبب حرمان بعض القوى والحركات من الحقوق السياسية أو عدم إشباع رغباتها وحاجاتها الأساسية وقد يوجه ذلك الإرهاب إلى الدولة أو النظام.

ه. أهداف اقتصادية: ويسمى الماركسيون هذا النوع من العنف اسم العنـف الطبقـي، أي ممارسـة الطبقة الغنية سيطرتها على الطبقات الفقيرة فتقوم الطبقة الفقيرة باستخدام العنف لإحداث تغييـر هيكلي في المجتمع.

و. دوافع انفصالية: إذ قد توجد بعض الأقليات التي ترغب بالانفصال عن المجتمع الذي تعيش فيـه والحصول على حكم ذاتي أو استقلال وانفصال فتقوم بالتعبير عن ذلك بعمليات إرهابية للضغط باتجاه انفصالها.

وأحياناً يكون الإرهاب الدولي واحداً من أنواع الصراعات التي قد تحدث قبل اسـتخدام السلاح النووي، وذلك إلى جاب الحرب التقليدية وحرب العصابات، ففي الحرب التقليدية وحرب العصابات يستهدف قتل أفراد القوات المسلحة وهذه هي طبيعة الحرب، بينما في الإرهاب فـإن القصد هو انتهاك المدنيين(بولتز وآخرون، 1999، ص15).

ويمكن القول أن عناصر الأنشطة الإرهابية المعاصرة تتشابه على الأغلـب فـي كافـة العمليات وهي(بولتز وآخرون، 1999، ص15-18):

أ- استخدام العنف من أجل الإقناع، أي لإقناع حكومة معينة والتأثير عليها لاتخاذ إجراءات معينة أو للتوقف عن اتخاذ إجراءات معينة.

ب- انتقاء الأهداف والضحايا للحصول على أكبر تأثير إعلامي.

ج- شن الهجمات دون التعرض للاستفزاز.

د- الحصول على أقصى دعاية بالتعرض لأقل المخاطر مثل أعمال التفجير التي تخلق كم كبير من الدعاية والانتشار تبعاً للتوقيت والمكان المختارين، وكذلك الاختطاف والاغتيال حيث يخلق قدر كبير من الدعاية والانتشار.

ه- استخدام عنصر المفاجأة للإحاطة بوسائل مكافحة الإرهاب.

و- استخدام التهديدات والإزعاجات والعنف لخلق جو عام من الخوف والتوتر مثل القيام بأكثر من عمل في آن واحد كزرع قنابل في حي كامل.

ز- عدم الانزعاج أو الاعتبار من استخدام النساء والأطفال كضحايا بل العكس قد يرغبون بأن يكون عدد النساء والأطفال أكبر لجعل الحادث أكثر ترويعاً.

ح- استخدام الدعاية لزيادة تأثير الهجمات خاصة ما يتعلق بالأهداف السياسية والاقتصادية.

ط- الولاء لأنفسهم أو للجماعات القريبة منهم.

وللتعرف على طبيعة الإرهاب بشكل أكبر، ومن حيث العلاقة بينه وبين الجريمة، تجد الباحثة أن هناك علاقة وطيدة بينهما، ويبرز ذلك من عدة نواحي كالآتي(بوادي، 2004، ص17-18):

أ. أهدافهما متشابهة تقوم على أساس واحد يتمثل بتحقيق مكاسب مادية أو سياسية بوسائل غير مشروعة.

ب. استخدام العنف والإرهاب ضد الأفراد والجماعات والحكومات.

ج. الاعتماد على تنظيمات سرية معقدة تضفي نوع من الرهبة والسرية على العمليات الإجرامية في ظل نظام دقيق وصارم لتنظيم عمل الجماعة والأفراد الداخلين فيها.

د. الطبيعة العابرة للحدود والوسائل غير المشروعة وغسل الأموال.

ه. وحدة التهديدات التي تظهر من تلك الجرائم التي تؤثر على الاستقرار الوطني والدولي وقيم الديمقراطية ودور القانون وحقوق الإنسان والتنمية الاقتصادية والاجتماعية.

و. نقل مركز النشاط إلى الخارج هروباً من الرقابة والمواجهة الأمنية لتنفيذ المخططات والإعداد والتدريب والتجهيز لتنفيذ الهجمات ومن ذلك استخدام أراضي الدول الأخرى لتلك الغايات.

ز. ارتباط الجماعات ببعضها خاصة القوية منها والمؤثرة والتي لها باع طويل في تلك الأنشطة غير المشروعة لتلقي التمويل والتدريب اللازم.

الفرع الثاني: خطر الإرهاب

يمكن تلمس خطر الإرهاب وآثاره من خلال المفاصل الرئيسية الآتية

أولاً: عنصر الخطر في الإرهاب

للخطر الجنائي صورتين: فقد يكون خطراً فعلياً يلزم توافره في الواقع المادي الملموس، وقد يكون خطراً مفترضاً لا يلزمه ذلك، ويعد الخطر بنوعية المبرر للتدخل التشريعي لحماية المصالح الاجتماعية قبل إلحاق الضرر بها.

وبالنسبة للخطر الإرهابي نجد أن تجريم الإرهاب، يقوم ابتداءً من خلال النظر إلى الخطر المتوقع منه، وكذلك الحال بالنظر إلى الضرر الذي قد ينجم عنه، وتأثيره على المصالح الاجتماعية التي يحميها القانون، ويتمثل عنصر الخطر في العمل الإرهابي في عملية استهداف بث الرعب في النفوس، والتأثير

والإضرار بقواعد النظام الاجتماعي واستقراره. لذا يمكن القول أن الخطر الإرهابي هو الفعل الكامن والصالح لإحداث ضرر جسيم لشخص أو لشيء ما، بهدف تقويض استقرار المجتمع وتوازن مصالحه، مستخدماً في ذلك العنف لإخافة النفوس أو بث الرعب فيها، بما يحدثه من أضرار جسيمة تدمر وتزلزل قواعد النظام العام والاستقرار الاجتماعي (حسني، 1964، ط2، ص110).

تجدر الإشارة في هذا الصدد أن الأعمال الإرهابية لا تستلزم استعمال وسائل من طبيعتها إحداث خطر عام، كما أن الخطر لا يهدد شخصاً أو أشخاصاً معينين، كما يرتبط التهديد غالباً باستعمال الأدوات الخطرة (محب الدين، د.س، ص199-200).

ويتميز الخطر الإرهابي ببعض العناصر كالآتي(بوادي، ص25-26):

أ. العنصر النفسي: وهو الخوف والرعب الناجم عن الاضطرابات النفسية التي تعتري النفس البشرية، بفعل الظواهر الخارجية عن الإنسان، والتي تلقي بظلالها على النفس الإنسانية محدثة خوفاً إذا كانت ضعيفة، أو تحدث رعباً إذا كانت تلك الاضطرابات شديدة.

ب. العنصر المادي: أي السيطرة والتسلط، وهو نتيجة للعنصر النفسي، لأن أعمال الرعب والخوف تمكن الفاعل من السيطرة على ضحاياه، لتنفيذ مخططه كاملاً، وتحقيق الأضرار بهم، وبالمحيطين بهم، وإفقادهم القدرة على المقاومة والدفاع، ومعرفة الجاني، وربما حتى رؤيته والحصول على أي معلومات تفيد عنه، وتفيد في ملاحقته وضبطه، وبالتالي التأثير على مصلحة المجتمع واستقراره.

ج. عنصر المباغتة والمفاجئة: لأنه يخلق نوع من التفوق الذي يساعد في السيطرة على الموقف وتنفيذ المخطط الإرهابي كاملاً ودون أي مقاومة من الضحية.

د. عنصر التخفي: وهي من مزايا الخطر الإرهابي، ومما ساعد في تسهيل التخفي عن أعين السلطات (بوادي، ص27):

1) المخترعات العلمية الحديثة التي تمكن الإرهاب من إخفاء مشاريعه وخطواته الإجرامية، عنـــدما يستخدم أجهزة التحكم عن بعد، واستخدام التقنية الحديثة بتزوير الوثائق وممارســـة الاتـــصالات بسرية تامة وعامل السرعة.
2) تماثل الإرهابيين مع عناصر المجتمع الأخرى فيصعب تمييزهم.

ثانياً: التخويف والذعر والحرب النفسية

يلتقي عنصر الذعر والخوف مع الحرب النفسية، باعتباره من عناصر الإرهاب، والحرب النفسية عبارة عن عمليات لتمرير معلومات منتقاة ومؤثرات لمستمعين أجانب، للتأثير على عواطفهم ومعتقداتهم ودوافعهم وتبريراتهم الموضوعية وسلوكياتهم، خاصة سلوك الحكومات الأجنبية والمنظمات والجماعات والأفراد. وتساعد العمليات النفسية في التأثير على النفسيات وإضعاف الروح المعنوية، وتخفيض فاعلية العدو، وهي بذلك جزء من النشاط السياسي والاقتصادي والمعلوماتي(البداينة، 2002، ص233).

بالتالي فإن العمليات النفسية قد تكون وسيلة من وسائل العمليات الإرهابية، والعكس صحيح، فالإرهاب قد يستعمل الحرب النفسية لتحقيق عنصر التخويف والذعر والهلع في النفوس كما قد بينا مسبقاً. إلا أن الباحثة ترى أنه لا يمكن اعتبار الحرب النفسية بحد ذاتها إرهاباً، وفي كل الأحوال، إلا إذا تحققت باقي العناصر في العملية الإرهابية.

ثالثاً: الأثر النفسي للإرهاب

عندما يوجه الإرهاب ضرباته في أوقات وأماكن مختلفة، فهو يكون قد أرسل رسالة إلى الحكومات وإلى الجمهور، أنه قادر على توجيه ضرباته أينما شاء، ووقتما شاء، وأن الحكومات ستكون عاجزة عن إيقافه (شريف، 1997، ص43).

فمن خصائص الأعمال الإرهابية أنها ترمي إلى إيجاد حالة من الذعر. وأنها ترتكب بوسائل تتعدى بنتائجها حالة الذعر والخوف، كتدمير المنشأة والسكك والمباني والجسور وتسميم المياه ونشر الأمراض المعدية والقتل الجماعي والخطف(محمد الجبور، 1993، ص274).

رابعاً: علاقة الإرهاب بالتنظيم أو الجريمة المنظمة

تعرف الجريمة المنظمة أنها:"تلك الجريمة التي يرتكبها عدد من الأشخاص المحترفين مستخدمين وسائل ومعدات علمية حديثة وأموالاً طائلة بتخطيط مدروس وتنظيم عالي، بقصد تحقيق أهداف اقتصادية"(صالح، 1998، ص275).

وترتبط الجريمة المنظمة بالإرهاب بسبب التشابه الجوهري فيما بينهما حتى أنه يسود الاعتقاد أن الإرهاب يعد أحد صور الجريمة المنظمة رغم اختلاف الدوافع والأهداف لكلا الجريمتين. حيث أن الإرهاب يهدف إلى احداث تغييرات سياسية أو اجتماعية أما الجريمة المنظمة فتهدف إلى تحقيق أرباح مادية وتحقيق أهداف اقتصادية (العازمي، 2007، ص73).

كما يرتبط هذا الأمر بمفهوم الإرهاب الإلكتروني أيضاً بشكل اوضح، خاصة في ظل التطورات الحديثة، إلا أن الباحثة تستهدف من هذا الأمر ربط الإرهاب بشقيه التقليدي والإلكتروني بمفهوم الجريمة المنظمة ابرازاً لخطر الإرهاب.

حيث أصبحت ظاهرة الإرهاب تمثل نوعاً من أنواع العنف المنظم، الذي ترتكبه الجماعات الإجرامية المنظمة، التي تهدد الأمن والاستقرار، وخاصة في ظل الإمكانيات التي سخرتها ثورة التكنولوجيا والمعلومات، وشبكة الإنترنت، ووسائل الاتصال الخارقة، الأمر الذي مكنهم من اقتراف أخطر الجرائم وأكثرها حرفة وتنظيماً، وبأدق الأسلحة المدمرة، ومن مسافات بعيدة، وبأقل جهد وأكثر سيطرة وأبعد عن الملاحقة.

ففي ظل التقدم العلمي والأنشطة والاستخدامات التكنولوجية غير المسبوقة، وبيانات الجنس البشري السرية وغير السرية، وفي كافة المجالات السياسية والاقتصادية والاجتماعية والعلمية والثقافية والفكرية، تطورت صور الإرهاب وأشكاله، وخاصة في ظل استخدام شبكات الإنترنت العالمية والمحلية، واستخدام وسائل الاتصال السلكية واللاسلكية عبر الأقمار الصناعية، واستخدام أنشطة البث والنشاط الإعلامي البالغ التطور، والتنوع التكنولوجي الذي جعل العالم قرية صغيرة، وكل ذلك ساعد على التمرد

على التقاليد والأوضاع الداخلية، الأمر الذي تسبب بعدم استقرار عالمي برزت مظاهره على مختلف أنشطة الحياة(بوادي، 2004، ص15). وصاحب ذلك ظهور عصابات الجريمة المنظمة، وتصاعدت وتيرة الأعمال الإرهابية في معظم دول العالم، وأخطرها الجرائم الإرهابية المنظمة.

خامساً: الأخطار والتهديدات الفضائية (الخطر في الإرهاب المعلوماتي)

من أنواع الخطر والتهديدات التي تبرز في اطار الإرهاب عامة والإرهاب المعلوماتي خاصة ما يأتي(البداينة، 2002، ص26):

أ. التهديد بالاضطراب في تدفق الاتصالات والتحويلات المالية والحملات المعلوماتية الهامة ومحطات الطاقة والمناقصات السياسية والاضطرابات في زمن الحرب، وهذا ما قد يؤدي إلى الخسارة والهزيمة.

ب. التهديد باستخدام المعلومات الحساسة والسرية وحق الملكية، لما لسرقة المعلومات أو الاحتيال بها من آثار سلبية على المستوى الفردي وعلى المستوى المؤسسي والمستوى الوطني.

ج. التهديد بانتقاء المعلومات لأغراض سياسية أو اقتصادية أو عسكرية واستغلالها في بعض المجالات أو تدميرها.

د. التهديد بتدمير المعلومات ومكونات البناء المعلوماتي التحتي الحساس ذات التأثير الكبير على الاقتصاد والأمن الوطني.

ومن الجرائم والتهديد في المجال الإلكتروني نرى بعض المفاهيم الجديدة مثل السرقة الإلكترونية والتجسس والإرهاب الإلكتروني أو الفضائي. ومن مظاهر الإرهاب الإلكتروني قراصنة الحاسب الآلي والدخلاء والمقتحمون الذين يحولون الانترنت إلى ساحة معركة، فهناك مثلاً مجموعة المنذرين

(Dispatches) التي أعلنت أنها ستدمر خادمات العرب والإنترنت في أفغانستان والدول الداعمة للإرهاب وقامت بحجز مئات المواقع منها للسفارة الإيرانية ومنها للمواقع الفلسطينية، وهناك مجموعة أخرى تسمى القراصنة الشباب (YIHAT) التي ادعت اختراقها بنوك إسلامية تدعم الإرهاب وأسامة بن لادن (البداينة، 2002، ص28). وأصبح الإنترنت ملاذاً آمناً للجماعات الإرهابية وعصابات الجريمة المنظمة والجواسيس، وأصبح بإمكان هؤلاء تنفيذ جرائمهم بأمان وعن بعد. وستتضح أهداف وأخطار الإرهاب المعلوماتي تباعاً، من خلال دراستنا التي تقوم على تناول هذا النوع من الإرهاب.

سادساً: الأثر الاقتصادي للإرهاب

وهذه الآثار الاقتصادية كالآتي (بوادي، 2004، ص19):

أ. التأثير على السياحة من خلال استهداف السائحين وإرهابهم ومنع الأنشطة السياحية وبالتالي التأثير على الأمن القومي.

ب. استهداف رجالات الدولة "رجال السياسة والفكر ورجال الدين وغيرهم".

ج. بعض العمليات الإرهابية تؤثر على الاقتصاد كتزوير العملة وتهريب المخدرات. وقد ساعد في ذلك وسائل الاتصال والانتقال والائتمان المتطورة.

د. التأثير على الحركة التجارية والاستثمارات الأجنبية بسبب الهجمات وأعمال العنف.

المبحث الثاني

الفضاء الإلكتروني وعلاقته بالإرهاب والجريمة المعلوماتية

بعد التعرف على مفهوم الإرهاب التقليدي من بعض وجهات النظر الفقهية والتشريعية حيناً، والدولية حيناً آخر، وبعض أحكامه وأسبابه وأهدافه والعوامل المؤثرة فيه بشكل عام، فإن الباحثة تنتقل في هذا المبحث للخوض بالإرهاب الإلكتروني الذي يعد محور دراستنا. حيث يعد هذا النمط الجديد من أخطر الجرائم التي تعاني منها المجتمعات، وصار نمطاً جديداً من أنماط الإرهاب، والأسهل ارتكاباً فيها، خاصة مع غزو التكنولوجيا الحديثة لكل مكان وسهولة الحصول عليها.

حيث باتت التكنولوجيا الحديثة تؤثر في الأمن الوطني وتشكل تهديداً واضحاً له وتفتح الباب أمام نمط جديد من الجرائم بشكل عام والإرهاب الإلكتروني بشكل خاص. بالتالي فإنه –وقبل البدء بتعريف الإرهاب الإلكتروني– يجب التعرف في محطة واحدة على ما هية التكنولوجيا الحديثة والبحث في العلاقة التي تربطها بالإرهاب كي يكون الانتقال تدريجيا للوقوف على ما هية الإرهاب الإلكتروني.

لذا فإن الباحثة تتناول هذا المبحث ضمن المطالب الآتية:

المطلب الاول: التكنولوجيا الحديثة وأثرها في الأمن الوطني

المطلب الثاني: أنواع الجرائم المعلوماتية وموقع جريمة الإرهاب الإلكتروني منها

المطلب الثالث: الربط بين الفضاء الإلكتروني والجرائم الإرهابية

المطلب الاول: التكنولوجيا الحديثة وأثرها في الأمن الوطني

طالما نحن بصدد الحديث عن التكنولوجيا الحديثة والبحث في علاقتها بالإرهاب، تمهيداً للوصول إلى مركز البحث وهو الإرهاب الاإلكتروني أو الفضائي، الذي يتم بمواجهة وسائل التكنولوجيا الحديثة أو بواسطتها، فإنه لابد من التعرف على هذه التكنولوجيا أولاً.

ويأتي ارتباط التكنولوجيا بالإرهاب من خلال أثر هذه التكنولوجيا ذا الوجهين، حيث جاءت بجوانب حسنة لا يمكن انكارها أو حتى الاستغناء عنها، بالمقابل لها جانب مظلم يتمركز تأثيره في الأمن الشخصي للأفراد، والأمن الوطني للدول والمجتمعات على السواء. ومن منطلق افتراض علاقتها بالإرهاب عامة والإرهاب الإلكتروني خاصة، فإنه لابد من البحث في تأثيرها على الأمن الوطني من جانب، ومن جانب آخر أنها تمثل محوراً في نمط آخر من الصراعات والجرائم، وهي حرب المعلومات التي ترتبط –كما سنرى– بشكل وثيق بالإرهاب الإلكتروني.

بالتالي فإن الباحثة تتناول ذلك من خلال الفرعين الآتيين:

الفرع الاول: التعريف بالتكنولوجيا الحديثة (الفضاء الإلكتروني)

الفرع الثاني: الثغرات الأمنية الجديدة والتهديدات المشتركة

الفرع الاول: التعريف بالتكنولوجيا الحديثة (الفضاء الإلكتروني)

تتعلق ثورة التكنولوجيا ابتداءً بالانترنت، وللانترنت تعريفات كثيرة، حيث تعرف أنها :"شبكة عالمية دولية ووسيلة من وسائل الاتصال والتواصل بين الشبكات، تجمع مجموعة من أجهزة الحاسب الآلي المرتبطة ببعضها البعض، إما عن طريق خطوط التلفون أو عن طريق الأقمار الاصطناعية وتعمل

وفقاً لبروتوكول (TCP/IP)، حيث تقدم للانسانية جملة من الخدمات كالبريد الإلكتروني وتبادل المعلومات"(إبراهيم، 2009، ص37. وهروال، 2007، ص6-7).

وتعني ثورة التكنولوجيا والمعلومات ذلك التطور الحاصل في نظم البيانات، والتطور الحاصل في مجال تقنية المعلومات، واختراع الحاسب الآلي والانترنت، حيث أدت هذه التطورات التكنولوجية إلى تقليل المسافات والجهود، وأحدثت ثورة فعلية في عالم الاتصال والمعلومات، وغزت العالم بأسره، حيث بات العالم غير قادر على تجاهلها، وتجاهل الآثار التي تزامنت معها، وغدا العالم لا يمكنه الاستغناء عنها، خاصة وانها دخلت كافة مناحي الحياة ومجالاتها.

ولهذه الثورة جانبين، جانب خير وجانب مظلم. فجانب الخير يتمثل بما قدمته ثورة الاتصالات والمعلومات بمساعدتها على عولمة المعلومات وتسهيل الخدمات والأعمال، حيث توصلت البشرية إلى السيطرة على المعلومات من خلال استخدام الحاسب الآلي، في عمليات تخزين ومعالجة واسترجاع المعلومات، واستخدامه في عمليات التصميم والتصنيع والتعليم والإدارة، وتطوير تطبيقاته لتشمل أداء كثير من الخدمات، كالتعليم، والتشخيص، والخدمات التمريضية، وتسهيل المعاملات والخدمات البنكية، والحجز الآلي لنقل الأشخاص، وغير ذلك من خدمات متنوعة، وبشكل عام دخل الحاسب الآلي في كافة مناحي الحياة الإنسانية، وجعل المعلومات متوفرة في متناول الجميع على شبكة المعلومات المحلية والإقليمية والعالمية (العادلي، 2009، ص2-3).

كما أصبح العالم بسبب الانترنت يزخر بكم هائل من المعلومات، ليس لها حواجز جغرافية ولا مسافات، حتى أن العالم اصبح شبيه بمجتمع كبير تربط الحاسبات وشبكات المعلومات أجزاؤه ببعضها، وهو ما يعرف ببزوغ فجر ثورة صناعية جـديدة أو ثالثة هي الثورة المعلوماتية، وبزوغ عصـر جـديد هو عصر المعلومات (رستم، 1994، ص5 وما بعدها. وسلامه، 2006، ص7).

أما بالنسبة للجانب المظلم، والمتمثل بالجرائم المعلوماتية بكافة أنواعها، والصور الأخرى لاستعمال الانترنت في افساد الثقافات، واعتباره بؤرة فاسدة تساهم في افشال وافساد الاخلاق وأسس التربية القويمة، وبؤرة مشجعة لفساد الاخلاق، وتعلم العادات السيئة. كما فتح المجال لنمط جديد من

الجرائم تعرف بالجرائم المعلوماتية، أو الجرائم الإلكترونية التي من بينها موضوع دراستنا –الإرهاب الإلكتروني.

الفرع الثاني: الثغرات الأمنية الجديدة والتهديدات المشتركة

بداية تشير الباحثة إلى مفهوم الأمن الوطني، الذي يعرف بأنه مجموعة من التهديدات الفيزيقية والتي ربما تواجه الدولة، وتدفع بالبنى والعقائد والسياسات العسكرية للتأهب لمواجهة هذه التهديدات. وهناك عوامل خارجية وداخلية مثل التغيرات الاقتصادية والاجتماعية التي ربما تؤثر بطريقة مباشرة أو غير مباشرة وتنقص أو تزيد من قدرة الدولة على مواجهة التهديدات الفيزيقية، والبعض يعرفه أنه الإدراك الجمعي للإحساس بالأمن(البداينة، 2002، ص21).

وهناك مفاهيم ترتبط بالأمن الوطني منها: الأمن الجماعي الذي يعرف بأنه قيام أعضاء في مجموعة محددة من الدول بنبذ استخدام القوة فيما بينها، والتعهد بالدفاع المشترك عن أي عضو في المجموعة يتعرض لتهديدات أو هجمات من أي طرف خارجي. وهناك الأمن الشامل الذي يشمل جميع الاحتياجات الإنسانية المهددة للبقاء على مستوى الفرد والجماعة والدولة والإقليم والكون. وهناك الأمن الإنساني الذي يشمل حماية الإنسان من تهديدات الجوع والمرض والقهر كإنسان(البداينة، 2002، ص21).

وقد شكلت جماعات على مستوى العالم سهل نشأتها وجود الإنترنت، تعمل على تكوين جماعات ضغط دولية تتواصل عبر الإنترنت، تمارس نشاطات عابرة للحدود تستهدف أنشطة في عدة مجالات من مجالات الأمن بشتى مفاهيمه.

كما يستفاد من الانترنت في المجال الأمني، فالانترنت ليست فقط مرتعاً للجرائم، حيث يقدم خدمات جليلة للعملية الأمنية، كتلقي البلاغات بصورة سريعة وفورية، واضفاء نطاق من السرية بين

الأمن والمتعاونين معهم لعدم تعريض حياتهم للخطر، واعطاء فرصة لمن لديه معلومات من الجمهور أن يقدمها بطريقة سرية دون تعريض أمنه وحياته للخطر، وتوسيع إطار البحث من خلال توزيـــع صـــور المجرمين ونشرها، كما يساعد في نشر المعلومات الأمنية المفيدة، والتواصل مع الجماعات الأهلية فـــي المجال الأمني، واصدار نشرات التوعية في المجالات الأمنية، وعمل الاستفتاءات اللازمة في المجـــالات المختلفة على الشبكة، ويسهل عملية الاتصال والتواصل بين الافراد والجهات المعنية في المجال الأمني، ويستفاد منه في المجال التعليمي والتدريبي في الموضوعات الأمنية (الجنبيهي منير والجنبيهي ممـــدوح، 2005، ص20-22).

ويرتبط الأمن بالمعلومات بشكل أساسي، لأن المعلومات ثروة يجب الحفاظ عليها وهي ذات قيمة عالية وثمينة تجعلها مصدراً للثروة في المجتمع، ويمكن استخدامها في شتى المجالات مما جعلها تـــصبح مستهدفة، وهذا ما جعلها تولد نموذجاً جديداً في المجال الأمني، فبعدما كان الصراع متعلقـــاً بالعناصـــر الأساسية للثروة والقوة والمال والمكانة، فقد أصبحت المعلومات تشكل بنية تحتية للمجموعات ومؤسساتها خاصة في ظل ازدياد الاعتماد على تقنيات المعلومات التي باتت مستهدفة، الأمر الذي جعـــل تهديـــدها تهديداً للأمن الوطني للمجتمع والدولة.

ومن هنا يمكن تعريف الأمن الوطني من منظور علاقته بالمعلومات وتأثره بها أنه: "الإحـــساس الجمعي الفعلي والتخيلي بعدم وجود و/أو تأثير التهديدات الفيزيقية والتخيلية لبنى المجتمـــع المعلوماتيـــة (خاصة الحساسة منها) في جوانبها العسكرية والاجتماعية والثقافية والاقتـــصادية وغيرهـــا"(البداينـــة، 2002، ص23).

أما عن تحديات أمن المعلومات فيمكن ايجازها بـــ:

1- عدم إمكانية السيطرة على الإنترنت وتحديده وتقييده بحدود الدول كما في الأمن التقليدي.

2- السرعة في انتقال التقنيات والمعلومات.

3- التحديات السياسية والاقتصادية والتكنولوجية.

4- التحديات التقنية.

5- التحديات الأمنية.

6- التحديات الوطنية كالتنمية والديموقراطية وحقوق الإنسان والتحدي البـشري ونقـص الكفـاءات والتحدي الثقافي والتربوي.

أما عن التهديدات الجديدة الناجمة عن المعلوماتية والفضاء الإلكتروني، فقد جـاءت المعلوماتيـة والتكنولوجيا الحديثة لتحقيق كثير من المزايا، التي أهمها التواصل والاتصال، وهذا ما جعل المعلوماتيـة هدفاً للحرب الجديدة أو حرب المعلوماتية، التي تشكل صورة أو نمطاً أو شكلاً مـن أشـكال الإرهـاب الإلكتروني، خاصة بعد أن أصبح العالم كله يعيش على التكنولوجيا والمعلوماتية، التي تشكل البنية التحتية لكل شيء، ومن مظاهر الاعتداء على المعلوماتية أو النشاطات العدوانية العمل على الحرمان من الخدمة، أو تعطيلها، أو استغلالها للمعلومات ونظم التشغيل وخدمات الاتصالات والمراقبة غيـر المـصرح بهـا للحاسبات، ونظم الاتصالات، وقطاع المعلومات، والتعديل غير القانوني أو التـدمير لرمـوز الحاسـب وبرامجه، وللشبكات، وتحوير المعلومات والخدمات المتعلقة بالحاسب أو الأقمار الصناعية مما يؤدي إلى خسائر كبيرة ومتعددة.

وتتعدد صور الاعتداء على البنية التحتية المعلوماتية وتتعدد الأهداف التـي تبتغـي مـن وراء الهجمات عليها وهي:

1. سرقة المعلومات عن خطط العدو وعن الاستراتيجيات السياسية والاقتصادية.

2. تعديل المعلومات وتغييرها وزرع معلومات خاطئة مكانها.

3. تدمير المعلومات ومسح المعلومات التي تشمل معلومات مالية أو عسكرية أو حكومية.

4. تدمير معلومات البنية التحتية من خلال الفيروسات.

وقد عبر مدير مركز حماية البيانات التحتي الوطني في مكتب التحقيقات الفيدرالية الأمريكي (ميشيل فيتس) عن المخاوف من التهديدات ومن الإرهاب الإلكتروني بقوله: "أن أدوات العدوان (الجريمة الفضائية) معقدة ومتوافرة لأي شخص يمكنه الوصول للإنترنت" (Girard ، Canada .(1998) .J.J. M S Infrastructure Vulnerabilities: New Role for DND Department of National .(p.iti، Peace and security wwwserver، War،Defense

كما مثلت التكنولوجيا والمعلوماتية تحدياً جديداً للأمن، مثلها مثل الصواريخ عابرة القارات والأسلحة المتطورة، وأحياناً تعد أخطر من ذلك، لسهولة الحصول عليها من كل شخص، وسهولة عمليات الهجوم كنشر الفيروسات والعمليات الأخرى.

وقد صنفت التهديدات إلى فئات كالآتي (البداينة، 2002، ص33-34):

1- التهديدات الخارجة المحايدة مثل التنصت وتحليل الإشارات وتحليل الذروات.

2- التهديدات الخارجية النشطة مثل الدخول غير المصرح به والحمولة الزائدة والازدحام.

3- الهجوم على نظام عامل.

4- الهجوم الداخلي.

5- الهجمات للوصول إلى تعديل النظام مثل خرق حماية الدخول للنظم، والانكشاف.

ومن خلال الاطلاع على الواقع الإجرامي في البيئة الإلكترونية، ووجود تلك التهديدات، يمكن القول أن هناك ثغرات كبيرة تتمثل في استهداف المعلوماتية التي تشكل أساس الحياة في الوقت الراهن، وتكاد تكون خطورتها أكبر وأكثر من خطورة الجرائم العادية، وتبرز الثغرات الفضائية والناجمة عن زيادة الاعتمادية على الاتصالات والمعلومات في المجتمع المعلوماتي، وزادت من احتمالية الاعتداء على البنية

التحتية، ويمكن القول أن كافة القطاعات أصبحت مستهدفة لاعتمادها على المعلوماتية، وهي قطاعات الاتصالات والمعلومات، وشبكات الاتصالات العامة، والإنترنت والحاسبات في المنازل، والاستخدام الأكاديمي والحكومي والتجاري، وقطاع التوزيع الفيزيقي الذي يشمل الطرق السريعة للمواصلات، وخطوط السكك الحديدية، والموانئ وخطوط المياه والمطارات، وشركات النقل وخدمات الشحن، وقطاع الطاقة الذي يشمل الصناعات التي تنتج الطاقة وتوزع الطاقة الكهربائية والبترول والغاز الطبيعي، وقطاع المال والبنوك الذي يشمل البنوك وشركات الخدمات المالية من غير البنوك. ونظم الرواتب، وشركات الاستثمار والقروض المتبادلة، والتبادلات الأمنية، وقطاع الخدمات الإنسانية الحيوية مثل: نظم التزويد بالمياه وخدمات الطوارئ والخدمات الحكومية(البداينة، 2002، ص36–37).

أخيراً تجدر الإشارة أنه وبالنسبة لطرق ارتكاب جرائم الحاسب الآلي عامة والتي يبنى عليها أيضاً أو يطبق هذا الوصف من خلالها على جرائم الإرهاب الإلكتروني هي(الجنبيهي منير والجنبيهي ممدوح، 2005، ص23):

أ. جرائم تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة

ب. جرائم تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها أو تدميرها كلياً أو جزئياً كالفيروسات.

ج. استخدام الحاسب الآلي كأداة لارتكاب الجريمة

د. اساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل أشخاص مرخص لهم استخدامه

المطلب الثاني: أنواع الجرائم المعلوماتية وموقع جريمة الإرهاب الإلكتروني منها

تعرف جرائم الانترنت بأنها الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الانترنت وبواسطة أشخاص على دراية عالية فيها (الجنبيهي منير والجنبيهي ممدوح، 2005، ص25).

وتسمى أيضاً جريمة نظم المعلومات وهي التي تتطلب اتلاف المعلومات أو اساءة استخدامها، وتعرف انها:"السلوك السيء المتعمد الذي يستخدم نظم المعلومات لاتلاف المعلومات أو اساءة استخدامها، فيتسبب أو يحاول التسبب، إما بالحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها"(داود، 2000، ص23.). ومن مصطلحات هذه الجريمة (أي جريمة نظم المعلومات: القرصنة والفيروسات والتسلل والاقتحام)

وهناك الكثير من التقسيمات والتصنيفات لجرائم الحاسب الآلي والانترنت، وقد أسهب الفقه في هذه التقسيمات كل حسب رأيه، وحسب الزاوية التي ينظر منها إلى هذه الجرائم، استناداً إلى كثير من المعايير، فمنهم من صنفها بناء على أداة الجريمة، ومنهم من صنفها حسب الجاني، ومنهم من صنفها حسب المجني عليه، ومنهم من اعتمد الحق المحمي فيها، أو المصلحة المحمية في هذه الجرائم كأساس لتصنيفها(سلامه، 2006، ص99).

ومن أبرز وأهم وأشمل التقسيمات للجرائم المعلوماتية، الاتجاه الذي قسمها إلى قسمين رئيسيين هما:

القسم الأول: جرائم المعلوماتية ضد النفس والأموال

القسم الثاني: جرائم المعلوماتية ضد المصلحة العامة وغيرها من الجرائم المعلوماتية الأخرى

وتتناول الباحثة هذه الاقسام في فرعين حسب هذا التقسيم هما الفرع الثاني والثالث. وقبل ذلك وفي الفرع الاول تتناول الباحثة التعريف بالجريمة المعلوماتية بشكل عام.

الفرع الأول: التعريف بالجريمة المعلوماتية

لقد فتح التطور التكنولوجي الحديث المجال لنمط جديد من الجرائم تعرف بالجرائم المعلوماتية، أو الجرائم الإلكترونية التي من بينها الإرهاب الإلكتروني. ومن هنا ارتأت الباحثة التعرف على مفهوم هذه الجرائم التكنولوجية أو الإلكترونية وآثارها، تمهيداً للبدء بالحديث عن الإرهاب الإلكتروني.

وتعد الجرائم الإلكترونية نوعاً من الجرائم المعلوماتية التي تعد ذات مفهوم أشمل، اذ تتمثل الجرائم الإلكترونية بشكل رئيسي في استخدام برامج الحاسب الآلي ونظمه لالتقاط بيانات ومعلومات معالجة إلكترونيا والتلاعب بأنظمة الحاسب التي تحتوي عليها، وذلك لأغراض غير مشروعة تتمثل غالباً بالسرقة والاحتيال، وباستخدام هذه البرامج والتعرف على نقاط الضعف في نظام الحاسب الآلي الخاص بالمجني عليه، فباستطاعة الجاني في هذا النظام السيطرة على نظام الحاسب بأكمله، ثم يقوم بنشاطه غير المشروع، ويحول هذا النشاط في النهاية إلى مكسب غير مشروع، وينتهي بمحو كل أثر يمكن أن يكشف عن أفعاله الاجرامية(سلامه، 2006، ص136).

وهناك عدة تعريفات للجريمة المعلوماتية، فمنهم من ضيق من نطاقها واعتبرها فقط تلك التي تتعلق بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابها ولملاحقتها وتحقيقها، واتجاه موسع يعتبرها كل فعل غير مشروع يتم بمساعدة الحاسب الآلي(سلامه، 2006، ص11-13).

فمنهم من عرفها أنها:"كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية" (عفيفي، 2003، ص32).

كما عرفها الفقيه الفرنسي (Massa) أنها:" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"(doc،www.arablaw/Download cyber crimes_General). كما عرفها البعض أنها:" فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو التي تحوّل عن طريقه" (عرب، موسوعة القانون وتقنية المعلومات، 1991، ص213).

والبعض عرفها أنها:" سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها" (القهوجي، 1992، ص172). وعرفتها منظمة التعاون الاقتصادي والتنمية OCDE أنها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية" (رستم، 1995، ص34).

أخيراً ترى الباحثة أنه يمكن تعريفها بأنها كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات، ونقل هذه البيانات. أو كل استخدام، يقع بصورة فعل أو امتناع عن فعل، غير مشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على أي مصلحة مشروعة سواء أكانت مادية أم معنوية.

كما تناولت عدة تعريفات الحاسب الآلي حيث عرف أنه:" جهاز إلكتروني يعمل طبقاً لتعليمات محددة سلفاً، ويمكنه استخدام البيانات وتخزينها والقيام بمعالجتها بدون تدخل الانسان ثم استخراج النتائج المطلوبة (أحمد، هلالي، 1997، ص16). وفي هذا الصدد تتناول الباحثة خصائص الجريمة المعلوماتية، وخصائص المجرمين المعلوماتيين، وأدوات الجريمة المعلوماتية.

وبالنسبة لخصائص الجرائم المعلوماتية، نجد أنها تتميز بالآتي (العالي، 2007، ص17. والسماك، 1992، ص68. وسلامه، 2006، ص95-98. والجنبيهي منير والجنبيهي ممدوح، 2005، ص14-15)):

أ. عادة لا يتم الإبلاغ عنها، إما لعدم اكتشاف الضحية لها، وإما لخشيته من التشهير به، ومما يدل على ذلك أن معظم جرائم الانترنت تم اكتشافها مصادفة وبعد وقت من ارتكابها، وأن عدد الجرائم التي لم تكتشف يعد أكثر بكثير من تلك التي تم اكتشافها(إبراهيم، 2009، ص86).

ب. نظرياً يسهل ارتكاب الجريمة المعلوماتية، وإخفاء معالمها، ومن الصعب اكتشافها وتتبع مرتكبيها. إذ تمتاز هذه الجرائم بصعوبة تحديد هوية مرتكبيها، وامكانية استخدام الشبكة لنشر الفكر الإرهابي والتطرف والعنف والتحريض عليهما، وهذا ما دفع الجماعات الإرهابية لإنشاء مواقع لها على الشبكة ترتكب جرائمها من خلالها.

ج. لا تترك الجرائم المعلوماتية أثراً لها بعد ارتكابها، كما أنه من الصعب الاحتفاظ الفني بآثارها إن وجدت، وتختلف بذلك عن الجرائم التقليدية، فآثارها أرقام تتغير في السجلات ومعلومات مخزنة إلكترونياً(إبراهيم، 2009، ص79).

د. تعتمد الجرائم المعلوماتية على الذكاء في ارتكابها، حيث تبين أنه يصعب على المحقق التقليدي التعامل معها، ومتابعتها، والكشف عنها، وإقامة الدليل عليها، لأنها جرائم تتسم بالغموض، وصعوبة الإثبات، والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية نتيجة لذلك.

ه. يتطلب اكتشافها الاستعانة بخبرة فنية عالية المستوى.

و. تسبب هذه الجرائم تشتت في الجهود المبذولة للتحقيق والتحري عنها بسبب عزلتها، ويصعب أيضاً التنسيق الدولي لتعقبها، حيث يمكن ارتكاب هذه الجرائم عن بعد، وقد يتعدد هذا المكان بين أكثر من دولة، ومن الناحية الزمنية تختلف المواقيت أيضاً بين الدول، الأمر الذي يثير صعوبة في تحديد القانون واجب التطبيق على ارتكابها.

ز. استغلال البريد الإلكتروني من قبل الإرهابيين لنشر أفكارهم والترويج لها، وتحقيق الاتصال بالاخرين والسعي لتكثير اتباعهم والمتعاطفين معهم.

ح. تمكين الإرهابيين من اختراق البريد الإلكتروني للآخرين، وكشف أسرارهم، والتجسس والإطلاع على معلوماتهم وبياناتهم، ومعرفة مراسلاتهم ومخاطباتهم، والاستفادة من ذلك في العمليات الإرهابية.

أما بالنسبة للجناة في هذه الجرائم، فإنهم أنواع كالآتي (إبراهيم، 2009، ص77. والعادلي، 2009، ص6):

أولاً: العاملون على أجهزة الحاسب الآلي في منازلهم، اذ بإمكان هذه الفئة الاتصال بأجهزة الحاسب الآلي، دون أن تتقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

ثانياً: الموظفون الساخطون على منظماتهم، حيث يقوم هؤلاء بالعودة إلى مقار عملهم بعد انتهاء الدوام، ويعمدون إلى تخريب الأجهزة أو اتلافها أو سرقتها، وقد يرتكب الموظف جريمة الحاسب الآلي أو الإنترنت صدفةً أو بدون تخطيط مسبق.

ثالثاً: فئة العابثين أو ما يعرفون بمسمى المتسللين (Hackers)، وتقع أغلب جرائم الإنترنت من قبل هذه الفئة، سواء الهواة منهم أو المحترفون، وهم نوعين:

- الهواة أو العابثون بقصد التسلية
- المحترفين اللذين يتسللون إلى أجهزة مختارة بعناية ويعبثون أو يتلفون أو يسرقون محتوياتها.

رابعاً: فئة العاملون في الجريمة المنظمة، كعصابات سرقة السيارات، حيث يستخدمون الشبكة في معرفة الولايات الأعلى سعراً من حيث قطع الغيار، ثم يقومون ببيع قطع غيار السيارات المسروقة في تلك الولايات.

وهم يتصفون بصفات عامة هي (العادلي، 2009، ص**6**):

أ. عادة ما تتراوح أعمارهم بين 18 إلى 46 سنة، ويكون المتوسط العمري لهم 25 عاماً.

ب. المعرفة والقدرة الفنية الهائلة.

ج. الحرص الشديد، والخشية من الضبط وافتضاح الأمر.

د. ارتفاع مستوى الذكاء، ومحاولة التخفي.

أما فيما يتعلق بأدوات الجريمة، فهي من المسائل الهامة في ظل دراسات القانون الجنائي، خاصة في مجال جرائم الحاسب الآلي والانترنت، إذ أنها أداة تختلف تماماً عن أداة الجرائم التقليدية، ومعظم أدوات الجريمة في مجال الحاسب الآلي والانترنت، تكون عادة موجودة ومتوافرة على الشبكة، ولا يمكن التخلص منها لأنها تستخدم في كثير من المجالات النافعة، فلا يمكن الاستغناء عنها، أو لعدم القدرة على السيطرة عليها أحياناً. ومن أمثلة ذلك أنه يوجد برامج لكسر كلمة المرور، لدخول الأجهزة المحمية بكلمة

مرور، في حالة أن ينسى مستخدم الجهاز كلمة المرور الخاصة به، ويطبق عليه برامج "CRACKING". وفي الوقت نفسه قد تستخدم هذه البرامج في فتح جهاز معين بعد معرفة كلمة السر والدخول إلى الإنترنت واستغلاله بشكل سيء.

بالتالي يمكن القول أن لهذه البرامج استخدامين نافع وضار، بالمقابل فإن الدول –خاصة الكبرى– تمتلك الوسائل والأدوات اللازمة لتعقب ومعرفة مصادر الفيروسات والهجمات التي تتم على البريد الإلكتروني والمواقـــــــع المختلفة الرسمية أو غير الرسمية. وهذا ما يفسر اهتمام مرتكبي الهجمات والاعتداءات بارتكاب جرائمهم من خلال أجهزة الآخرين (السند، 2005، ص32–33).

الفرع الثاني: جرائم المعلوماتية ضد النفس والأموال

ونتناول هنا الجرائم ضد النفس أولاً، والجرائم ضد الأموال ثانياً.

أولاً: الجرائم المعلوماتية ضد النفس

تعرف الجرائم ضد النفس أو جرائم الاعتداء على الأشخاص، أنها الجرائم التي تنال بالاعتداء، أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحت، أي الحقوق اللصيقة بشخص المجني عليه، والتي تعد من مقومات الشخصية، وتخرج لأهميتها الاجتماعية، وما يجب أن تحاط به من احترام عن دائرة التعامل الاقتصادي، وهي بطبيعتها غير ذات قيمة متبادلة (حسني، 1988، ص317).

ومن هذه الحقوق: الحق في الحياة، والحق في سلامة الجسم، والحق في الحرية، والحق في صيانة العرض، والحق في الشرف والاعتبار. ومن الجرائم التي تمثل اعتداء على هذه الحقوق: جرائم القتل، وجرائم الايذاء، وجريمة الإجهاض، وجرائم الاعتداء على العرض: كجرائم الاغتصاب، وهتك العرض، والزنا، وجرائم القذف والسب، وجريمة البلاغ الكاذب، وجريمة إفشاء الأسرار.

وليس بالإمكان ارتكاب هذه الجرائم جميعها من خلال الحاسب الآلي أو شبكة الانترنت، إلا أنه يمكن ارتكاب بعضها، كنلك الجرائم التي يمكن أن يستخدم فيها الحاسب أو الانترنت أساساً، ومن هذه الجرائم مثلاً: القتل بالحاسب والتسبب في الوفاة (؟)، وجرائم الإهمال المرتبط بالحاسب، والتحريض على الانتحار، وقنابل البريد الإلكتروني، وأنشطة ضخ البريد الإلكتروني غير المرغوب به، وجريمة انتهاك حرمة الحاسب أو الدخول غير المصرح به، وجريمة تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم بأنشطة جنسية عبر الوسائل الإلكترونية، وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة، وتلقي أو نشر المعلومات عن القاصرين عبر الحاسب من أجل أنشطة جنسية غير مشروعة، والتحرش الجنسي بالقاصرين عبر الحاسب والوسائل التقنية (العادلي، 2009، ص7–8)، وهناك كثير من هذه الجرائم التي يمكن ارتكابها ضد الحاسب الآلي أو بواسطته.

ثانياً: الجرائم المعلوماتية ضد الأموال

الجرائم ضد الأموال بشكل عام هي: الجرائم التي تنال بالاعتداء، أو تهدد بالخطر، الحقوق ذات القيمة المالية، ويدخل في نطاقها كل حق ذي قيمة اقتصادية، ويدخل تبعاً لذلك في دائرة التعامل، وأحد عناصر الذمة المالية(حسني، 1988، ص 803).

ويمكن تصور ارتكاب مثل هذه الجرائم في نطاق المعلوماتية، ومنها مثلاً: سرقة معلومات الحاسب، وقرصنة البرامج، وسرقة خدمات الحاسب ووقته، وسرقة أدوات التعريف والهوية عبر انتحال الصفات أو المعلومات داخل الحاسب، وتزوير البريد الإلكتروني أو الوثائق والسجلات والهوية، وجرائم المقامرة، والجرائم الأخرى ضد الأخلاق والآداب، وتملك وإدارة مشروع مقامرة على الانترنت، والحيازة غير المشروعة للمعلومات، وإفشاء كلمة سر الغير، وإساءة استخدام المعلومات، واغتصاب الملكية، وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات، وإدخال معطيات خاطئة أو مزورة إلى نظام حاسب، والتعديل غير المصرح به بالكمبيوتر، وجرائم الاحتيال بالتلاعب بالمعطيات والنظم، واستخدام

الحاسب للحصول على البطاقات المالية أو استخدامها للغير دون ترخيص أو تدميرها، والاختلاس عبر الحاسب أو بواسطته، واستخدام الانترنت لترويج الكحول ومواد الإدمان للقصر.

الفرع الثالث: الجرائم المعلوماتية ضد المصلحة العامة وغيرها من الجرائم المعلوماتية

ونتناول أولاً جرائم المعلوماتية ضد الحكومة والجرائم الأخرى من جرائم المعلوماتية ثانياً.

أولاً: جرائم معلوماتية ضد الحكومة

يقصد بهذه الجرائم بوجه عام تلك الجرائم التي تنال بالاعتداء، أو تهدد بالخطر الحقوق ذات الطابع العام، أي تلك الحقوق التي ليست لفرد أو لأفراد معينين بذواتهم، فالحق المعتدى عليه فيها هو المجتمع بمجموع أفراده، أو هو الدولة باعتبارها الشخص القانوني الذي يمثل المجتمع في حقوقه ومصالحه كافة (حسني، 1988، ص11).

ومن أمثلة هذه الجرائم: جرائم الاعتداء على الأمن الخارجي أو الداخلي للدولة، والرشوة والاختلاس، وتزييف العملة، وتزوير المستندات الرسمية. ويمكن أن تقع هذه الجرائم بواسطة الحاسب الآلي والانترنت ومنها: تهديد السلامة العامة، والعبث بالأدلة القضائية أو التأثير فيها، وبث البيانات من مصادر مجهولة، وجرائم تعطيل الأعمال الحكومية، وجرائم تعطيل تنفيذ القانون، وجرائم عدم الإبلاغ عن جرائم الحاسب، والحصول على معلومات سرية، الأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات (العادلي، 2009، ص9)، وأخيراً من أهم هذه الجرائم جرائم الإرهاب الإلكتروني موضوع دراستنا.

ثانياً: الجرائم الإلكترونية الأخرى

تتعلق هذه الجرائم على الأغلب بخدمة الانترنت وتزويدها وما يتعلق بها كخدمة وتقديمها، ومن أهم هذه الجرائم مايلي(العادلي، 2009، ص9-11):

- جرائم أسماء نطاقات الإنترنت: والتي تتصل بالنزاعات حول أسماء نطاقات الانترنت، حيث تثير مسألة أسماء النطاقات إشكاليات تقنية تستوجب الحل، من أبزها كم عنواناً يلزم إضافته؟ وأي من هذه العناوين تشمله الحماية القانونية؟ وهل العنوان الذي استخدم بالفعل أم العنوان الذي تم حجزه بهدف الاتجار فيه؟ ومن الذي يتحكم بهذه العناوين؟ ومن يبيع العناوين الجديدة؟ أو بالأحرى من له الحق في بيع هذه العناوين؟ ومن الذي سيفصل في النزاعات التي ستنشأ بمناسبة هذه العناوين؟ وما الحل إذا تم بيع العنوان لأكثر من شخص أو جهة؟.
- جرائم مزادات الانترنت: وهي جرائم الاحتيال عبر مزادات متعددة الصور أبرزها: الاحتيال وعدم التسليم أو التوصيل، والاحتيال وخداع المشتري حول القيمة الحقيقية للصنف المعروض للبيع، وتجارة بضائع السوق السوداء، والمزادات الصورية، وجرائم مزودي الخدمات.

وهناك تقسيم آخر يحتل أهمية واسعة في ظل تلك التصنيفات، ويعد من أشهر هذه التصنيفات وأهمها، وهو التصنيف الوارد في مشروع القانون النموذجي الأمريكي لجرائم الكمبيوتر والانترنت لعام 1998، الموضوع من قبل فريق بحثي أكاديمي، والمسمى (Model State Computer Crimes Code)، حيث قسم هذه الجرائم إلى (عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص11):

- الجرائم الواقعة على الأشخاص
- الجرائم الواقعة على الأموال عدا السرقة
- جرائم السرقة والاحتيال
- جرائم التزوير
- جرائم المقامرة
- الجرائم ضد الآداب، عدا الجرائم الجنسية
- الجرائم ضد المصالح الحكومية

وبموجب هذا التقسيم الذي جاء استناداً إلى فكرة الغرض النهائي، أو المحل النهائي الذي يستهدفه الاعتداء. فإن جريمة الإرهاب الإلكتروني تعد من بين جرائم الكمبيوتر المرتكبة ضد الحكومة. وتشمل طائفة جرائم الكمبيوتر المرتكبة ضد الحكومة، كافة جرائم تعطيل الأعمال الحكومية، وتنفيذ القانون، والحصول على معلومات سرية، وبث البيانات من مصادر مجهولة. كما تشمل الإرهاب الإلكتروني، والانشطة الثأرية الإلكترونية، أو انشطة تطبيق القانون بالذات (عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص13).

المطلب الثالث: علاقة الفضاء الإلكتروني بالإرهاب

لا يُعّد العنف الصفة الأساسية للإرهاب، إنما وسيلة لتحقيقه، وهناك كثير من المواقف والحروب فيها عنف ولا تعد إرهاباً، إنما ينصرف العنف إلى وسيلة لبث الرعب والفزع بين جموع الـشعب، لأن غاية الإرهاب وصفته الأساسية هو نشر الرعب والفزع والخوف (فرانـك تـولتز وآخـرون، 1999، ص13). وهذا ما يربطنا بمفهوم الدراسة، أو يربط مفهوم الإرهاب بالفضاء الإلكتروني. إذ أن الفـضاء الإلكتروني يعد وسيلة لنشر الفزع والرعب والخوف في كثير من الأحوال، وربما بشكل أسرع وأسهل من وسائل نشر الذعر والرعب في الإرهاب التقليدي.

وهذا ما يدفعنا إلى دراسة الآليات التي يتم من خلالها الاعتداء على البنية التحتية المعلوماتية، والتي يشكل الإرهاب الإلكتروني واحداً منها:

1. الأفراد سواء الموظفون والأفراد العاملين داخل المنظمات الرسمية والخاصة أو أفراد المجتمـع، حيث يمكن استغلال المعلومات وتخريبها أو تعديلها أو سرقتها لمختلف الأهداف.

2. المعدات والأدوات: ومنها البنادق الاشعاعية ذات الترددات الإشعاعية العالية، والتي تؤدي إلـى الحرمان من الخدمة، من خلال توجيه إشارات إشعاعية عالية على أهداف محددة مسبقاً، ودوائر كهربائية عرضة لأن تحمل حمولة كهرومغناطيسية زائدة مما يؤدي إلى تعطلها. وهنـاك قنابـل إرسال النبض الكهرومغناطيسي، والتي تعد أكثر قوة من البنادق لدرجة أنهـا تعطـل الـدوائر والشرائح في الحاسب، والمعلومات المخزنة بحيث لا يمكن إصلاحها، وتعمـل علـى تخريـب الأدوات الاتصالية والتحرش بالخصم، وتعطيل الاتصالات، والتدمير، والتخريـب، والإرهـاب، والدفاعات الأرضية والجوية، وتدمير المعدات الإلكترونية (البداينة، 2002، ص44).

3. الإرهاب: سواء أكان إرهاباً تقليدياً يعمل على تدمير البنية التحتية للمعلومات كالمباني، وأجهـزة الحاسب، وتعطيل المواصلات. أم إرهاباً تكنولوجياً كالذي يهدف إلى التـأثير علـى الفـضاء، باستخدام وسال مادية مثل: تفجير محطات الطاقة والاتـصالات التـي تـؤثر علـى الفـضاء

الإلكتروني، أو الإرهاب الذي يدمر البرمجيات، والمعلومات، ويشمل ذلك الفئات الآتية(البداينة، 2002، ص45):

- التعدي الفضائي على قاعدة معلومات محددة، كالدخول غير الشرعي على الشبكة، أو النظام بهدف تحويل أموال بطريقة غير مشروعة، وسرقة ممتلكات معلوماتية وتحطيم الملفات.
- الاعتداء الفضائي بهدف الحصول على وصول وولوج إلى الشبكة والاستفادة من إجراءات الأمن واستغلال ثغراتها.
- التجسس.
- غلق النظام.
- التعليمات المؤذية مثل المنطقية وحصان طروادة لتدمير البرمجيات.

وقد يستخدم الإرهابيون الشبكة الكونية في إجراء اتصالاتهم وعملياتهم واستغلال المواقع، كالمواقع الإباحية لإخفاء معلوماتهم، واستخدام تقنيات مختلفة لحماية معلوماتهم كالتشفير. كما أن المعلوماتية تسهل على الإرهابيون الحصول على المعلومات والبرمجيات التي تساهم في تنفيذ الأعمال الإرهابية، كتصميم الأسلحة وتحضير الأسلحة البيولوجية(البداينة، 2002، ص45).

4. الإرهاب المعلوماتي: ويتمثل ذلك بصورتين: فقد تكون تقنية المعلومات هدفاً للإرهابيين، وقد تكون هدفاً للإرهاب بقصد التخريب الإلكتروني أو المادي، وتدمير نظم المعلومات، وأية بنية تحتية معلوماتية، هذا من جانب ومن جانب آخر عندما تكون تقنية المعلومات أداة لعمليات كبيرة تشكل اللجوء للإرهاب، واستغلاله لأنظمة معلومات وسرقة بياناتها لتنفيذ عملياته (البداينة، 2002، ص46).

وللانترنت وظائف معينة تساهم أو تساعد في الإرهاب الإلكتروني، ويمكن ايجازهـا بـــ (نظمـي، 2010، ص19):

أولاً: الاعلام: وتبدو الوظيفة الإعلامية من خلال التعبئة المعنوية، وتحريض المناصـرين والمؤيـدين، والقيام بالحملات الإعلامية والحرب النفسية. حيث تقوم الجماعات الإرهابية باستغلال دور الاعلام فـي تنفيذ الأعمال الإرهابية، حيث قد يساعد الإعلام بقصد أو بغير قصد الإرهاب،عندما تقوم وسائل الاعلام بتغطية أخبار العمليات الإرهابية والاجرامية، فإن الإرهابيين يحققون أهـدافهمن فـي جـذب الاهتمـام والترويج لمطالبهم، ونشر الذعر والخوف لدى المواطنين والفئات المستهدفة. ومـنح الإرهـابيين وقتـاً للتخطيط عند صعوبة تحديد هوية مرتكبي الجرائم الإرهابية، والناجمة عن البلبلـة الإعلاميـة، وتبـاين وتناقض الأخبار المتعلقة بالأعمال الإرهابية. والتأثير على مصير الضحايا والرهائن سلباً وإيجاباً (نظمي، 2010، ص17).

ثانياً: الاتصال والتنسيق: حيث يتم ذلك من خلال التنسيق والاتصال بين أعضاء المجموعات من خـلال توظيف فنون وأساليب التشفير.

حيث يهتم الإرهابيين أو مرتكبي الجرائم الإرهابية بنوعيهـا التقليـدي والإلكترونـي عمومـاً، بتكنولوجيا الاتصالات التي تستخدم في الحياة اليومية، إذ أن هذه الوسائل تحسن من الاتصالات، وتساعد على تدفق الدعم والمساعدات، وتسمح للأعضاء بالتنسيق فيما بينهم بشكل أسرع، كما أنها تشكل وسـيلة للدعاية لهم للوصول إلى جمهور ضخم من المانحين وتجنيد الاعضاء في مـساحات جغرافيـة واسـعة (المراغي، 2002، ص17).

ثالثاً: استخدام الإرهابيين جرائم الانترنت كوسيلة لتحقيق الأهداف الإرهابية

حيث يهدف الإرهابيون إلى تحقيق نتائج غير مشروعة من خلال أعمال غير مشروعة، ويتمثل هدف الإرهابيون -كما سبق وأن أشارت الباحثة- بإثارة الذعر والرعب، وتحقيق السيطرة والتأثير على أصحاب القرارات، ويمكن القول أن هذا الهدف يمكن تحقيقه من خلال جرائم الانترنت، استناداً إلى خصائص هذه الجرائم، وعلى حجم الضرر الذي تحدثه، بالتالي فإن في هذه الجرائم سمات تغري الإرهابيين لاتخاذها وسيلة لتحقيق أهدافهم الإرهابية (العالي، 2007، ص17).

رابعاً: التعليم والتدريب: من خلال توظيف كافة خدمات وبرامج الحاسب والانترنت في ذلك، وتبادل الأفكار حول طرق تضليل رجال الأمن، وكيفية صناعة الأسلحة والمتفجرات وغير ذلك من عناصر تدريبية يمكن اتمامها من خلال الشبكة.

ويستفيد الإرهابيون من الانترنت من خلال انشاء مواقع على الشبكة تمكنهم من نشر أفكارهم، والدعوة إلى مبادئهم، وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، ومن هذه المواقع التي أنشأها الإرهابيون، مواقع لتعليم صناعة المتفجرات، ومواقع لتعليم كيفية اختراق المواقع وتدميرها، ومواقع لتعليم طرق اختراق البريد الإلكتروني، ونشر الفيروسات والدخول إلى المواقع المحجوبة أو المحظورة. ومن المظاهر التي يساعد فيها الانترنت ويرتبط فيها بشكل مباشر بالإرهاب: التعرف على أساليب الإرهاب والتخريب وتعلم البعض لها من الانترنت. والتعرف على المواقع التي تشجع وتساند الإرهاب والمشاركة فيها. وامكانية تعلم بعض العمليات أو الوسائل الإرهابية من الشبكة ككيفية صناعة القنابل. وتعلم بعض المظاهر السيئة من الانترنت كتعلم طرق الانتحار. وتنمية بعض المهارات والأساليب التخريبية ككيفية نشر الفيروسات وتدمير وسائل الاتصال مع المحترفين "الهاكرز"(نظمي، 2010، ص16-17).

بالتالي يمكن القول أن من سلبيات الانترنت في مجال الإرهاب، أنه يمكن من معرفة كيفية صناعة المتفجرات وتهريبها وتداولها والتعامل معها، ويعلم كيفية صناعة القنبلة النووية. كما أنه يمكن من غسيل الأموال وتبييضها، أي أنه يرتبط بجريمة غسيل الأموال والتي يمكن أن تتم بطرق إلكترونية كما سنرى. كما أنه يسهل عملية سرقة البطاقات الائتمانية، أي أنه مرتبط أيضاً بجريمة سرقة البطاقات الائتمانية.

ومما يغري الجماعات الإرهابية وأفرادها في ارتكاب جرائم الإرهاب الإلكتروني، تلك الخصائص

التي تحققها الوسائل التي يتم من خلالها ارتكاب هذه الجرائم، وما تختص به من: عدم وضوح للجريمة، وصعوبة إثباتها، وصعوبة التوصل إلى الجناة، وإمكانية حدوثها في زمن قصير، وصعوبة كشف وتحديد وقت ارتكابها (الزيدي، 2003، ص58).

تجدر الإشارة في هذا الصدد إلى دور الصورة المرئية في الإرهاب، وذلك أن الفضاء الإلكتروني يتضمن بطياته نموذجاً للصورة المرئية، وهي ليست الصورة المرئية التقليدية المتمثلة بالتلفزيون، إنما هي تلك التي تتم من خلال الانترنت، إلا أن تأثير الصورة المرئية وعلاقتها بالإرهاب تتساوى بشكل عام إن كانت تلك القادمة من التلفزيون أم من الانترنت.

لقد اصبح للصورة (المرئية) في زمن العولمة والقرية الكونية الواحدة وعصر الفضاءات المفتوحة تأثير مباشر على المجتمع، من خلال ما يعرض وما يشاهد على شاشات التلفزة، حيث أصبح التلفزيون والصحافة الإلكترونية يكتسحان كل وسائل الاعلام الأخرى من حيث القراءة والاستماع المتداولة عالمياً وإقليمياً ومحلياً، أو من حيث توسع شبكات الاعلام في الانتشار الحقيقي أو في الايرادات الاعلانية، ومع تطور تكنولوجيا العلوم وعلوم الاعلام والاتصال أصبحت الصورة التلفزيونية هي سيدة التعبير ومالكة النظر والسمع والانتباه والفكر الواعي واللاواعـــــــــي. وتتمتع الصورة التلفزيونية بقدرة كبيرة على استحواذها على اهتمام المتلقي وحواسه (حجازي، عبد الفتاح، 2009، ص17-18).

ويؤثر الاعلام المرئي في الإرهاب بشكل مزدوج من حيث تأثير الصورة وتأثير الكلمة، فهو الوسيلة الوحيدة التي تعتمد الطبيعة التلازمية لثنائية الصوت والصورة في نقل المضمون الاعلامي، وهو وسيلة لإنصاف المتعلمين لفهم ما يدور حولهم وبناء معارفهم الموجودة أساسياتها لديهم(علوان، 2008، ص37)، وقد أثبت الاعلام المرئي نجاحه وكلما زاد تأثيره على حواس المتلقين زاد نجاح الوسيلة في تحقيق أهدافها، ويزداد دوره كل يوم في حياة الناس، لأنه يهدم الفواصل بين الحقيقة والوهم ويتمتع بتقنيات إغراء ووصول إلى المتلقي ويساعد في ترسيخ نظام من الأوليات في مجتمع ما حول مشاكله وأهدافه، كما أنه يسجل الماضي ويعكس رؤية الحاضر ويؤثر في المستقبل، وهذا ما جعله الوسيلة الجماهيرية الأهم والأقوى والأكثر تأثيراً في المشاهدين وفي نطاق دراستنا كان هناك برنامج يسمى (حوار العرب)

عرضته الفضائية العربية ونشرت تفاصيله العربية نت، كان قد خصص حلقته ليوم 2008/5/8 لمناقشة موضوع الاعلام والإرهاب بمشاركة متخصصين يعملون في مراكز الدراسات والبحوث في كل من القاهرة وعمان وواشنطن، ودار خلاله مناقشات تركزت حول المؤسسات الاعلامية ومسؤولية العاملين فيها والقائمين عليها في ما يتعلق بالترويج للإرهاب أو الحد منه، وفي استفتاء تم اجراؤه للطلبة المشاركين في البرنامج على الهواء مباشرة، تناول الاجابة على ثلاث اسئلة وقد أكدت اجابات معظم المشاركين بنسبة (48%) على أن التلفزيون هو الوسيلة الإعلامية الأكثر نشراً للدعاية الإرهابية (علوان، 2008، ص38).

كما أن التلفزيون قادر على استخدام الصوت والصورة بطريقة فعالة وفريدة عبر الخطاب المباشر للمشاهدين، الذين سيجدون فيه أنفسهم وجهاً لوجه مع من يتحدث اليهم مباشرة على شاشة التلفزة، كما أنهم يمتلكون اتصالاً بصرياً وهمياً بالمتحدث، بالتالي يمكن تلمس تأثير العنف الذي يحدثه التلفزيون على المشاهدين، لأن العنف الذي نشهده في التلفزيون يرتبط بالعنف في المجتمع، وهذا لا يعني أن العنف فقط من التلفزيون لكن يعد التلفزيون من الأمور التي تساعد في ذلك إلى جانب بعض العوامل الأخرى التي تؤثر بالعنف بشكل مباشر ورئيس وهي: الأمية، والبطالة، والتطرف الديني، والصراع السياسي.

وفي هذا الصدد نشير إلى احصائية أمريكية جرت في بداية التسعينيات أثبتت أن خمسة عشر فيلماً بوليسياً عرضها التلفزيون قد اشتملت على اربعمائة وست جرائم وحشية، وأن التلفزيون يعرض من الجرائم ما يعادل عشرين مرة بقدر الجرائم التي تحدث في الحياة الاعتيادية، ومع ذلك فهناك من يرفض فكرة الربط بين التلفزيون والإرهاب لعدم وجود دليل علمي كاف يثبت أن التغطية الاعلامية التي يقوم بها التلفزيون تحفز بالفعل على الإرهاب، لأنه بات من العسير تحديد الأعمال التي توصف بأنها إرهابية والتي لا يمكن أن تثار حولها ضجة اعلامية، ومع ذلك فقد ثبت أن الإرهاب لا يمكن أن يترعرع دونما رعاية أو دعاية ، حيث أن تمجيد النشاطات الإرهابية يتم من خلال توفير تغطية شاملة لها. فقد يمنح التلفزيون مساحة زمنية منه لعرض الإرهابين وما يقومون به وتوفير التغطية الاعلامية اللازمة لهم وعرض حوادث اختطاف الطائرات ومحاصرة السفارات وعرض أي حدث إرهابي، وهذا ما يشجع على

تكوين جماعات إرهابية جديدة تحاول الاستفادة من التغطية المجانية التي يقوم بها التلفزيون للنشاطات الإرهابية (حسن علوان، 2008، ص41).

المبحث الثالث

التعريف بالإرهاب الإلكتروني وحرب المعلومات

عرفنا فيما مضى معنى ومفهوم وخطر الإرهاب التقليدي، وعلاقته بالعالم والفضاء الإلكتروني، وتأكيداً على ذلك وجدنا أن المعلومات قد تكون وسيلة لتنفيذ الإرهاب التقليدي فيصبح إرهاب بوسائل إلكترونية بصرف النظر عن النتيجة التي تظهر عن الأعمال الإرهابية، وقد تكون هدفاً للعمليات الإرهابية فيكون إرهاباً يستهدف أكثر من هدف ومن هذه الأهداف المستهدفة نظم المعلومات والمواقع الإلكترونية وشبكات الاتصال السلكي واللاسلكي وكل ما فيه فضاء إلكتروني ووسائل إلكترونية وقد يكون الإرهاب إلكتروني كحرب المعلومات، أي تنفيذ عمليات إرهابية إلكترونية ضد جماعات أو بين جماعات مختلفة فقط من خلال الوسائل الإلكترونية دون الاختلاط بالإرهاب بمفهومه التقليدي.

وتتوجه الباحثة هنا إلى الصورة الأخيرة والتي تكاد تجمع بين طياتها الصورتين السابقتين، بالتالي فإننا نركز عليها لأنها تشمل الوسائل الإلكترونية كحرب متبادلة أم غير متبادلة، بصرف النظر عن وسائل مباشرة العمليات، أو إذا كانت الأهداف تقليدية أو إلكترونية.

وتزداد أهمية موضوع الدراسة عندما نرى العالم اليوم يخشى الأفراد والجماعات أكثر من خشيته من الدول ومما زاد أهمية تلك الجماعات وسهل عليها تنفيذ عملياتها التطور التكنولوجي الذي دخل جميع مناحي الحياة وغير صورها وصار بالإمكان استخدامه لتنفيذ جرائم إرهابية تقليدية وصار بالإمكان استخدامه لخلق الذعر والإرهاب والترويع وسواء أفضى إلى نتيجة مادية ملموسة أم بقي على مجرد الخطر. بالتالي فإن الدراسة والتركيز سينصب على عنصر المعلومات الإلكترونية وعلاقته بالإرهاب، حيث يتم ذلك من خلال المطلبين الآتيين:

المطلب الأول: التعريف بالإرهاب الإلكتروني وأسبابه

المطلب الثاني: الإرهاب الإلكتروني وحرب المعلومات (الحرب الإلكترونية)

المطلب الأول: التعريف بالإرهاب الإلكتروني وأسبابه

ظهر الإرهاب الإلكتروني كصورة جديدة من صور الإرهاب، تلك الجريمة التي يعاني منها العالم بأسره، في ظل ظهور تكنولوجيا الحاسب الآلي والانترنت، وزيادة اعتماد العالم عليها، فلم يعد يحتاج الإرهابي ذو الخبرة الاحترافية في هذا المجال الحيوي والإلكتروني المعقد، سوى جهاز حاسب آلي وتأمين اتصاله بشبكة الإنترنت للقيام بأعمال تخريبية وإرهابية، وهو جالس آمن في بيته أو عمله أو حتى في مقهى، وذلك من خلال بعض النقرات البسيطة على لوحة المفاتيح، أو باستخدام الفارة، ودون أن يترك أثراً أو دليلاً في الفضاء الذي يتعامل به ليدل عليه.

فبدخول التكنولوجيا الحديثة –الانترنت والحاسب الالي– تغير مفهوم الإرهاب من مجرد اعتباره اعتداء على شخص ما وإصابته بأذى فعلي أو ذعر أو تهديد، وزالت الحدود بين المفهومين القديم والإرهاب الإلكتروني، حيث أصبح الإرهاب الإلكتروني يشكل تهديداً كبيراً، وصار من السهل اقتحام صفحة أو موقع ما، ونشر تهديدات من خلاله، واقتحام بعض المواقع الهامة، كاقتحام مواقع البورصة العالمية وأنظمة الاتصالات، والكهرباء والمياه والمواصلات والطيران، والشبكات الحكومية، وشبكات الأمن. وللإرهاب الإلكتروني أهمية خاصة لدى بعض الجماعات لأن الانترنت مجال مفتوح وواسع، وليس له حدود، ويتوسع كل يوم، ويمكن الوصول اليه من أي مكان وفي أي بلد بتكاليف بسيطة (الصيفي، 2008، بدون رقم صفحة).

ويتم التعرف على الإرهاب الإلكتروني في هذا الموضع من الدراسة من خلال تعريفة أولاً في (الفرع الاول) وبيان أسبابه وأهدافه في (الفرع الثاني).

الفرع الأول: التعريف بالإرهاب الإلكتروني

يتمثل الإرهاب بصورة عامة بكونه يمثل اعتداء على أمن الدول الداخلي والخارجي على السواء، وتتخذ جرائم الإرهاب طابعاً دولياً يميزها، الأمر الذي يبرر الاهتمام الدولي بها، من حيث قيام الدول بعقد اتفاقيات بشأنها، وتوفير نوع من الاطار التشريعي الملائم في التشريعات الوطنية. وفي هذا الصدد نجد أن

لهذه الجرائم –اي الإرهابية– تأثير على الانترنت، ويمارس الإرهاب فيها من خلال عدة صور وأفعال قد تعد جرائم مستقلة بذاتها متى تم التعامل معها بشكل منفرد، إلا أنها قد تكون أفعالاً إرهابيةً في المجال الإلكتروني. ومن ذلك التجسس واختراق الأنظمة الأمنية للدول على الانترنت (بن يونس، 2004، ص645).

ويظهر الإرهاب في كثير من المجالات لعل ابرزها مجال علاقة السلطة السياسية بالجماعات المعارضة لها، كما يظهر لتحقيق كثير من الأهداف والغايات، ومنها أهداف سياسية، كما يمثل انتهاكا للقواعد القانونية والشرعية العامة، والقواعد العرفية والدينية السائدة في المجتمع، من خلال اشاعته للاحساس بعدم الامان في المجتمع (التل، 1998، ص11).

وينصرف مصطلح الإرهاب كما تبين مسبقاً إلى الأفعال الاجرامية الموجهة ضد الدولة، والتي تهدف إلى إثارة الرعب العام لدى شخصيات معينة أو مجموع الأشخاص أو الوسط العام، بالتالي فإنه – وحسب الرأي الفقهي– تعد السمة البارزة فيه عنصر التخويف والترهيب والترويع، سواء من حيث طريقة استخدام الوسائل المؤدية إلى ذلك بطبيعتها أو عن طريق التهديد باستخدامها، أياً كان الغرض منها طالما كان غير مشروع من الناحية القانونية (العناني، 1992، ص134). ويتخذ الإرهاب الإلكتروني أشكالاً متعددة تختلف عن أشكاله في العالم المادي، كونها تقتصر على ما فيه من تخويف ولكن بأسلوب رقمي.

ويعرف الإرهاب الإلكتروني أنه :"تعبير يشمل مزج مصطلح التهديد بنظم المعالجة الآلية للمعلومات باستخدام تقنية الاتصالات الحديثة: الانترنت"(Dorothy E Dening، 2000، available http://www.cs.geoegetown.edu/~denningat: من: عمر بن يونس، 2004، ص649). ولا يشكل التهديد بحد ذاته إرهاباً، لأنه لا يعد جريمة طالما لم يخرج إلى العالم المادي، إلا أنه بالنسبة للجرائم الإرهابية فيجب توافر عنصر الترويع والتخويف والازعاج، ومن هنا يأتي الربط بين الإرهاب وكثير من الجرائم التي قد تعد قائمة بحد ذاتها كالتخريب والاتلاف والقتل، والإرهاب عبر الانترنت واثارة الفتن العرقية والداخلية فهي جرائم تقع ضمن دائرة الإرهاب، لأنها تعبر عن استفزاز طوائف معينة وخلق نزاعات بين الاعراق.

وقريباً من عنصر التهديد أيضاً عرف البعض الإرهاب الإلكتروني أنه:" العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفـراد علـى الإنسان: بدينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق، بشتى صنوفه وصـور الإفـساد فـي الأرض" (السند، 2004م، ص8).

وبشكل أوسع ورد تعريف له في الموسوعة الحرة، أنه:"استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو القيام بمهاجمة نظم المعلومات لدوافع سياسية أو عرقية أو دينية"(ويكيبيديا الموسوعة الحرة، بدون رقم صفحة). وتعد الشبكة العنكبوتية ذات أهمية بالغة في مجال ارتكاب الجرائم الإرهابية، اضـافة إلى الأغراض البحثية التي أنشئت لأجلها، وهذا ما دفع وكالات المباحث والاستخبارات المركزيـة فـي الولايات المتحدة في أعقاب احداث سبتمبر الشهيرة للحصول على حريات أكبر في تعقـب المعلومـات الرقمية.

ويميز البعض بين الإرهاب الإلكتروني وتكنولوجيا الإرهاب، والتي تعني :" جملة الأنشطة العقلية الموجهة والمهارات التي يستخدمها الإرهاب للكشف عن خصائص معطيات بيئته المحيطة والتعامل معها بالتوظيف والاستغلال للمعطيات المعينة له في تحقيق هدفه أو التكيف مع المعطيات المعيقة له في تحقيق ذلك الهدف باستخدام المواد والأدوات والتجهيزات وتطوير المهارات" (نظمي، 2010، ص14).

ومن التعريف يتضح أن لتكنولوجيا الإرهاب جانبين هما:

- الجانب المادي الذي يتعلق بالمواد التي يستخدمها الإرهاب أو الإرهابي للنقل والاتصال أو الأسـلحة المستخدمة سواء كانت أسلحة خفيفة أو متفجرات أو أسلحة كيميائية وبيولوجية.

– الجانب المعنوي الذي يتعلق بالمعارف والخبرات والمهارات والأساليب اللازمة لتعامل الإرهابي مـع البيئة المحيطة، واستخدام أو تصنيع الجانب المادي من تكنولوجيا الإرهاب.

ويمكن القول من خلال التعريفات أن ظاهرة الإرهاب الإلكتروني أو الرقمي عبارة عن نوع آخر من الإرهاب، جاء نتيجة التطور التكنولوجي والثورة المعلوماتية، وإستغلال شبكة الإنترنت للهدم والتخريب. ويلاحظ أيضاً أن الإرهاب الإلكتروني يتخذ جانبين هما(المصري، د.س، بدون رقم صفحة):

- استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين. أي استخدام التكنولوجيا وسيلة للإرهاب بشكله التقليدي.
- مهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية أي استخدام التكنولوجيا أو جعلها هدفاً ومحلاً للجريمة الإرهابية.

وقد ظهر الارتباط الوثيق بين الإنترنت والإرهاب بشكل واضح وجلي بعد أحداث الحادي عشر من سبتمبر الشهيرة عام 2001، حيث انتقلت المواجهة ضد الإرهاب والإرهابيين من المواجهة المادية المباشرة إلى المواجهة الإلكترونية، كما تحولت الحروب من الواقعية إلى الرقمية. فقد أدى ظهور الحاسبات الآلية وانتشارها وظهور الانترنت، لتغير شكل الحياة في العالم، وأصبح من السهل اليسير الحصول على وسائل تقنية المعلومات الحديثة، واستخدامها في غير الجوانب التي جاءت لأجلها.

تلاحظ الباحثة من التعريفات المتقدمة أن الإرهاب الإلكتروني هو الإرهاب التقليدي ذاته، لكن مع تغير في الوسيلة التي يتم من خلالها تنفيذ الركن المادي لجريمة الإرهاب، أو تغير في محل الجريمة، إذ أن السمة البارزة التي تميز الإرهاب بشكل عام هي عنصر التخويف والترويع وبعض العناصر الأخرى التي لا تتعلق بالمحل أو بالوسيلة.

فالتكنولوجيا والتقنية الحديثة قد تكون وسيلة لارتكاب جريمة الإرهاب، وقد تكون محل الجريمة وهدفها، فقد تقع اعتداءات على التقنية ذاتها تمثل نوعاً من أنواع الإرهاب وصوره، منها القرصنة والاغراق وانتهاك الخصوصية، وان كانت تمثل بذاتها جرائم مستقلة وتمثل نوعية حديثة من الجرائم إلا أنها في أحوال معينة قد تعد من ضمن الصور والأفعال الإرهابية متى تحققت شروط معينة لاعتبار الجريمة إرهابية.

وبالمقارنة مع تعريفات الإرهاب التقليدية يمكن القول أن الإرهاب الإلكتروني عبارة عن الاعتداء أو التهديد به مادياً أو معنوياً، باستخدام وسائل إلكترونية، يصدر من الدول أو الجماعات أو الأفراد على السواء، ويمثل اعتداء على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله. أو يكون إرهاباً محله الفضاء الإلكتروني.

الفرع الثاني: أسباب الإرهاب الإلكتروني وأهدافه

قد تتشابه أهداف وأسباب الإرهاب الإلكتروني، باعتبار أن السبب الذي دفع إلى ارتكاب الجريمة يمثل الغاية التي يتوخاها الإرهابيون من أفعالهم وجرائمهم، وبشكل رئيسي يمكـــن القـــول أن الإرهـــاب الإلكتروني مثله مثل الإرهاب التقليدي، يهدف إلى زعزعة الأمن ونشر الخوف والرعب وإختلال النظام العام للدول، وتهديد وابتزاز الأشخاص والسلطات العامة والمنظمات الدولية، والسطو وجمـــع الأمـــوال، وجذب الانتباه، والدعاية والإعلان (مهران زهير المصري، د.س، بدون رقم صفحة).

يمكن بداية الإشارة إلى أسباب الإرهاب الإلكتروني للتعرف على مـــدى العلاقـــة التـــي تـــربط التكنولوجيا بواحدة من أهم وأخطر الجرائم التي ترتكب، وتحتل مساحة واسعة من الخطر ومـــن الآثـــار السلبية على المجتمع المحلي والدولي.

وييمكن تبويب أسباب الإرهاب الإلكتروني من قبل الباحثة كالآتي:

أولاً: من أسباب الإرهاب الإلكتروني، ما يتعلق بالمؤثرات الجرمية أو التي تساعد في ارتكاب الجريمة أو التي تتسبب بها. حيث نجد أن جميع المؤثرات يمكن توافرها من خلال الإنترنت، فلـــه طبيعـــة الأرض، يساعد ويسهل في الاختفاء والاختباء، وتدمير الآثار والأدلة، ويوفر مناخـــاً جيـــداً للتخطـــيط للعمليـــات الإرهابية، وهو غذاء كامل ومتكامل لها، وله تأثير على عقول البعض كتأثير الخمور عليهـــا، ويتـــسبب أحياناً في إثراء العنصريات، وزيادة النقص الحاصل في الألفة بين الناس، ويشغل أبناء الطوائف الذين لا يجدون نقابات لهم للتجمع من خلال المنتديات والمواقع الإلكترونية ومواقع التواصل الاجتماعي، كما أن ترك الشباب بدون الاشتراك بالعملية السياسية يدفعهم باتجـــاه الإنترنـــت، والانجـــراف وراء القنـــوات الإرهابية، خاصة في ظل ضعف أنظمة القضاء والدفاع وأجهزة الرقابة، ويتشابه ذلك مع حرص الشباب باعتبارهم طائفة هامة من الشعب من المشاركة في الحياة السياسية بإبداء الرأي مـــن خـــلال الاســـتفتاء الشعبي.

ثانياً: ويعود السبب في ظهور الإرهاب الإلكتروني، وتطور مظاهر الإرهاب المختلفة، إلـى الثـورات العلمية والتكنولوجية التي هيأت المجال الخصب لإحداث تغيرات متنوعة على كافة المستويات وفي كافة المجالات. ففي مجال الجريمة والإجرام استفاد المجرمون من معطيـات العلـم والتكنولوجيـا، ونظـم المعلومات والاتصالات المتطورة، الأمر الذي ساهم في ظهور القلاقل الاجتماعية والسياسية التي تحدث في مختلف دول العالم، فظهر كثير من الجرائم التي لم نكن نسمع بها من قبل مثل: جرائم الحاسب الآلي والانترنت والجرائم المعلوماتية(بوادي، 2004، ص16).

ثالثاً: ومما يساعد في ارتكاب الإرهاب الإلكتروني صعوبة الرقابة على الانترنت أو المحاسبة على مـا ينشر فيه، وهذا ما جعل الانترنت مقراً للإرهابيين. حيث يجذب الانترنت المنظمات لافتقـاره لعناصـر الرقابة، كما أنه بيئة مناسبة لممارسة الأعمال الإرهابية ونشر الأفكار المتطرفة التي تسيطر على وجدان الأفراد وإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعـارض ومـصلحة المجتمع، أو القيام بأعمال تخريبية بشكل يخفي هويتهم المباشرة، بطريقة أسهل وأبسط ممـا يقـوم بـه الإرهابيون التقليديون حيث يحتاجون أسلحة ومدرعات وقنابل وتحركات سرية وتكاليف ماديـة، بينمـا يحتاج الإرهاب الإلكتروني فقط إلى بعض المعلومات ليستطيع اقتحام الحواجز الإلكترونيـة، بتكـاليف بسيطة لا تتجاوز جهاز حاسوب والدخول إلى الشبكة العنكبوتية. والآن نجد المواقع الإرهابيـة تتطـور بسرعة خارقة من حيث التصميم والإمكانات التقنية، ويمتاز الإرهابيون بقدرة وخبرة عاليتين في استيعاب نظم وبرامج الإنترنت واستغلالها في تطوير تقنياتهم وتوظيفها في تحقيق غاياتهم.

ويتميز الإرهاب الإلكتروني بأن له وجود نشط متنوع ومراوغ بصورة كبيرة على الشبكة، حيث يظهر ويختفي ويعاود الظهور بشكل وعنوان إلكتروني جديدين، كما تتوسع وتتنوع أهدافه والمجالات المستهدفة من قبل منفذيه، وامكانية توفير السلامة للمعتدي، وتنفيذ أهدافه بجهد قليل وعدم التعرض لخطر اكتشاف هويتهم.

وترتبط أسباب الإرهاب الإلكتروني بمجموعة من العوامل التي يمكن ايجازها كالآتي (الفتلاوي، 2005، ص93-94):

أولاً: العامل النفسي، وهو المعبر عن مدى تأثير العمل المنفذ في نفوس الأفراد، فإن فقد هذا الجانب فلا يعد العمل الممثل للعنف إرهاباً، ويرتبط هذا العامل بالعامل المادي، فالخوف هو نتيجة حتمية ومرتبطة بالفعل. وترى الباحثة إمكانية تحقيق العامل النفسي بالوسائل الإلكترونية وذلك من عدة جوانب: إذ أن استخدام الإنترنت قد يؤدي إلى خلق العامل النفسي، من خلال تخوف مستخدمي الشبكة من ولوج الجماعات الإرهابية التي تستخدم الشبكة إلى بعض المواقع الخاصة، وانتهاك الخصوصية من جهة، ومن جهة أخرى أنه يمكن استخدام الإنترنت لغرض العمليات الإرهابية، للتأثير في نفوس الآخرين وخلق الذعر والرعب لديهم. وسيتم تناول هذه العمليات بنوع من التفصيل بشكل متقدم من دراستنا.

ثانياً: العامل الاجتماعي، ويقصد من العمل الإرهابي التأثير بالمجتمع ككل وليس بالضحية. وهذا ما يمكن القيام به- برأي الباحثة- أو تحقيقه من خلال الشبكة العنكبوتية، ومواقع التواصل الاجتماعي إذ أنه يمكن استخدام تلك المواقع التي بمتناول الجميع لتحقيق العمليات الإرهابية أو عرض آثارها على تلك المواقع بشكل يحقق غايات الجماعة أو التنظيم الإرهابي.

ثالثاً: العامل المادي، أي استخدام القوة المسلحة أو العنف السياسي، وفي مجال الإرهاب الإلكتروني يمكن اعتبار وجود العامل المادي من خلال استخدام الإنترنت لتنفيذ العمليات الإرهابية والتخطيط لها، أو المساهمة بتنفيذ تلك العمليات بأي شكل كان.

رابعاً: العامل السياسي، أي أن تهدف العمليات إلى تحقيق أغراض سياسية.

خامساً: عامل الضعف، ويعني ذلك أن العمل الإرهابي يعبر عن ضعف الجماعة في تحقيق غايتها بالطرق الأخرى. وقد يظهر ذلك – برأي الباحثة- من خلال تخوف الجماعة واستخدامها للإنترنت، للقيام أو المساهمة بالقيام بالأعمال الإرهابية من خلال التخفي في آفاق الفضاء الإلكتروني.

سادساً: ديمومة العمل الإرهابي، أي إبقاء المجتمع في حالة تأهب مستمر تحسباً لوقوع عمليات إرهابية. ويممكن اعتبار وجود هذا العامل بصرف النظر عن وسيلة الإرهاب إن كانت إلكترونية أم لا، حتى أنـــه من الممكن من خلال الانترنت، تحقق هذا العامل بشكل أكبر، حيث أن الإنترنت قد غزا البيوت، ويكـــاد يكون الجميع متمكناً من الدخول إليه، أو الحصول عليه بأقل الأسعار، فيبقى العالم علـــى تواصـــل مـــع الأحداث أولاً بأول ومترقباً لها، بالتالي فإن البيئة الإلكترونية تساهم إلى حد كبير بتحقيق هذا العامل.

المطلب الثاني: الإرهاب الإلكتروني وحرب المعلومات (الحرب الإلكترونية)

يزداد اعتماد العالم على المعلومات يوماً بيوم ودخلت المعلوماتية في كافة المجالات والميـادين، وظهرت بذلك الثورة المعلوماتية وهي ثورة اجتماعية أصابت تغييراتها كافة الـنظم الاجتماعيـة، ولـم تقتصر آثارها على الاتصالات والمواصلات بل تعدت ذلك إلى العلاقات الإنسانية وكافة مناحي الحيـاة. كما تعد المعلومات ذات قيمة عالية في أوقات السلم والحرب على السواء ويتم استخدامها في كل الوقـت لأهميتها، ولا يقتصر أثرها على مجرد المعلومة وجمع المعلومات، بل أصبحت أداة فعالة في تحقيق كثير من الأهداف فهي الآن من أهم أهداف الحرب لما لها من أهمية.

ويرتبط الإرهاب الإلكتروني بالحرب الإلكترونية من عدة وجهات نظر، فمن جانب يقـوم كـل منهما على المعلوماتية، وهذه السمة الجديدة الغالبة لحروب اليوم إن كنا نتحدث في إطار الإرهاب الدولي، والسمة الغالبة لجرائم اليوم إن كنا نتحدث عن الإطار الوطني، إذ نجد الآن أن غالبية الجـرائم أصـبح للانترنت والتكنولوجيا الحديثة علاقة بها، سواء أكان من أدوات الجريمة، أو هدفاً لها، أو وسائل مساعدة فيها، وحتى أنها قد تكون أحياناً دليلاً أو قرينة تساعد في اكتشاف الجرائم وتعقب مرتكبيها.

وفي إطار حديثنا عن الإرهاب الإلكتروني، الذي قد يتخذ الصفة الدولية – دون تعميق الفصل بين النوعين– إذ اننا نتحدث ونبحث في الإرهاب الإلكتروني، أياً كان نوعه أو مستواه، دولياً أم وطنياً، فإنـه من المناسب التعرف على الحرب الإلكترونية أو حرب المعلومات، وبيان علاقتها بالإرهاب الإلكتروني، وهي علاقة متبادلة كما سيتضح لنا تباعاً، فالإرهاب الإلكتروني قد يكون وسيلة مـن وسـائل الحـرب المعلوماتية، وقد تكون الحرب المعلوماتية وسيلة للإرهاب الإلكتروني.

لذا فان الباحثة تتناول هذا المطلب من خلال الفروع الآتية:

الفرع الأول: التعريف بحرب المعلومات

الفرع الثاني: علاقة حرب المعلومات بالإرهاب الإلكتروني

الفرع الأول: التعريف بحرب المعلومات

لا يوجد تعريف محدد ودقيق لمفهوم الحرب الإلكترونية، بالرغم من اجتهاد عدد من الخبراء في تقديم تعريف لها حيث عرّفها كل من (ريتشارك كلارك) و(روبرت كناكي) أنها:" أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها" (P.6، 2010، Richard A. Clarke،Robert knake).

وتعني حرب المعلومات ذلك الوصف لحرب المستقبل المرتبطة بعصر المعلومات رغم أن جذورها عميقة وكانت تستهدف عقل الإنسان. وهي صراعات تتضمن حماية المعلومات وانتقائها وتخريبها والحرمان من استخدامها والسيطرة عليها والتحكم بها. بالتالي فهي استخدام للمعلومات في تحقيق الأهداف والمصالح الوطنية. كما تعني حرب المعلومات تخريب المعلومات أو تدميرها أو سرقتها أو تحريفها أو إساءة استخدامها أو المنع من الوصول إليها أو تقليل موثوقيتها أو استخدامها ضد أصحابها(البداينة، 2002، ص154).

وتعد الحرب الإلكترونية من صور الإرهاب الإلكتروني وترتبط بها بشكل رئيس، حيث يتم هذا النوع من خلال ما يعرف بهجمات الشبكات الكمبيوترية، وهي من أنواع الحرب الإلكترونية أيضاً وهي المفهوم الأعم والأشمل، وتستهدف هذه الحرب اتخاذ إجراءات تؤثر بشكل سلبي على المعلومات ونظمها، وتتضمن هذه الحرب بعض الأنشطة مثل: أمن العمليات، والعمليات النفسية، والخداع العسكري، الهجمات الفيزيائية، والهجمات على شبكات الكمبيوتر. وتنفذ هذه الحرب من خلال هجمات رقمية، منها: الهجمات المباشرة التي تتم من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات الهامة ضمن شبكاته، باستخدام القوة العسكرية المباشرة. وسرقة المعلومات من أجهزة الخصم، وتخريب قواعد البيانات الخاصة به والتلاعب بها. واستخدام الفيروسات وبعض الأساليب الرقمية الأخرى. ويلاحظ أن هذه الصور تتشابه مع صور وأشكال الإرهاب الإلكتروني (ويكيبيديا الموسوعة الحرة، بدون رقم صفحة).

ومن خصائص حرب المعلومات: أن مدخلاتها قليلة التكلفة، ولا تتطلب كلفة مادية كبيرة أو دعم حكومي كبير كما هو الحال في الحرب التقليدية. وتتمتع بحدود تقليدية غير واضحة. ودور متنامي لإدارة

الإدراك. وتحدي استراتيجي جديد للاستخبارات. وضعف التحذير التكتيكي المرعب وتقدير التعدي حيث لا يوجد نظام تحذير تكتيكي مناسب للتمييز بين هجمات حرب المعلومات الاستراتيجية والهجمات الأخرى لنشاط الحيز الفضائي بما في ذلك التجسس. وصعوبة بناء تحالفات دائمة والحفاظ عليها، إذ أن الاعتمــاد على تحالفات يمكن أن يزيد الثغرات الأمنية لجميع الشركاء إلى هجمات حرب المعلومات الإستراتيجية. وأخيراً تلاشي الحدود الجغرافية وانكشاف الأراضي (البداينة، 2002، ص149).

في هذا الصدد تجدر الإشارة إلى بعض أسلحة الحرب الإلكترونية وهي الفيروسات المعروفة في مجال الفضاء الإلكتروني، ومن أحدث هذه الأسلحة في مجال الحرب الإلكترونية فيــروس (ستكــسنت)، حيث ادعت ايران في 2010/9/25(Robert McMillan، Was Stuxnet Built to Attack Iran's Nuclear Program?، 2010)، أن العديد من وحداتها الصناعية وقعت ضحية إرهاب إلكترونــي بعــد إصابتها بفيروس "ستكسنت"، الذي يعد واحداً من أعقد الأدوات التي تم استخدامها، وهو عبارة عن برنامج كومبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحــدات التــي تعمل آلياً، بعد أن كان الخبراء يعتقدون أن مهمّته هي التجسس الصناعي ونقل المعلومات لتقليد المنتجات. إلا أنه تبين فيما بعد خلاف ذلك، وأنه عبارة عن نوع جديد من البرامج التي من الممكن أن تتحول إلــى نموذج للأطراف التي تنوي إطلاق هجمات إلكترونية يمكن أن تتسبب بدمار حقيقي واقعــي فــي البلــد المستهدف حتى بدون الحاجة إلى الإنترنت(Mark Clayton، Staff writer، 2010).

ويعمل البرنامج بشكل محدد جداً، حيث يقوم بإختراق الأجهزة والحواسيب، ثم التفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة "سيمنز الألمانية"، فإذا ما وجدها يقوم عندها بتفعيل نفسه، ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة، من خلال العبث بأنظمة التحكم، ويمكن أن يهاجم كثير من المنشآت كخطوط نقل النفط ومحطات توليد الكهرباء والمفاعلات النووية وغيرها، وإذا لم يجد تلك العلامة الفارقة فإنه يترك الحاسوب وشأنه. ويعد هذا البرنامج من البرنامج الكبيرة والمشفّرة والمعقدة، ويوظّف تقنيات ذكية وجديدة، ويعمل بدون تدخل بشري. ولهذا السبب فإنه يعمل بشكل محدد جداً، وهذا ما يدفع للقول أنه من صنع دولة وليس من صنع شخص منفرد، ومن جانب آخر فهو يهاجم المنشآت الأساسية التي يكون هناك قيمة وميزة من تدميرها. وقد تم اكتشاف "ستكسنت" لأول مرة من قبل شركة بيلاروسية

تدعى VirusBlockAda التي عثرت عليه في جهاز كمبيوتر يعود لأحد عملائها الإيرانيين، إلا أن الاتهام اتجه نحو روسيا، أو الصين، أو أمريكا أو اسرائيل (باكير، 2010، ص5–6).

الفرع الثاني: علاقة حرب المعلومات بالإرهاب الإلكتروني

من خلال ما تقدم نجد أن الحرب الإلكترونية أو حرب المعلومات عبارة عن مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني، وقد يكون لها طابع دولي. ومن جانب آخر تبين أن الإرهاب الإلكتروني يقع في مستويات النزاعات التي تتم في الفضاء الإلكتروني، إلا أنه يقترب من مفهوم آخر أو شكل آخر من الحرب الإلكترونية لا يكون الفاعلون فيه حكوميون، وهي من صور الحرب الإلكترونية وحرب المعلومات إلى جانب القرصنة والتجسس.

وللتعرف على علاقة الإرهاب الإلكتروني بالحرب الإلكترونية أو حرب المعلومات، نجد أنها علاقة تبادلية نوعاً ما، وتتضح من خلال إيجاز صور الحرب الإلكترونية. وترتبط صور هذه المنازعات، بالإرهاب الإكتروني، الذي يعد بذاته جانب من جوانب حرب المعلومات والحرب الإلكترونية، ومن هذه النزاعات أو صور الحرب الإلكترونية (باكير، 2010، ص1):

- القرصنة أو التخريب الإلكتروني: وتقع في المستوى الأول من النزاعات التي تتم في الفضاء الإلكتروني، وتتضمن هذه العمليات القيام بتعديل أو تخريب أو إلغاء محتوى. ومن أمثلتها ما يعرف باسم الملقّمات (Servers) حيث يتم إغراقها بالبيانات فتتم عملية القرصنة.
- الجريمة الإلكترونية والتجسس الإلكتروني: وهما المستوى الثاني والثالث، وغالبا ما يستهدف هذان النشاطان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.
- الإرهاب الإلكتروني: ويقع في المستوى الرابع من النزاعات التي تتم في الفضاء الإلكتروني، ويستخدم مصطلح الإرهاب الإلكتروني لوصف الهجمات غير الشرعية التي تنفّذها مجموعات أو فاعلون غير حكوميون (Non-State Actors) ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزّنة،

ولا يمكن اعتبار أي هجوم إلكتروني بأنه إرهاب إلكتروني، إلا إذا انطوى على نتائج تؤدي إلى أذى مادّي للأشخاص أو الممتلكات والى خراب يترك قدراً كبيراً من الخوف.

- الحرب الإلكترونية: وهي المستوى الأخطر من مستويات النزاع في الفضاء الإلكتروني، وتعد جزءاً من الحرب المعلوماتية بمعناها الأوسع، وتهدف الحرب الإلكترونية إلى التأثير على إرادة الطرف المستهدف السياسية، وعلى قدرته في عملية صنع القرار، والتاثير في القيادة العسكرية وتوجهات المدنيين في مسرح العمليات الإلكتروني، وبسبب خصائص هذه الحرب، فمن المتوقع أن تصبح نموذجاً تسعى إليه العديد من الجهات، ومن هذه الخصائص:
- أن حروب الإنترنت هي حروب لا تناظرية (Asymmetric) بسبب التكلفة المتدنية نسبياً للأدوات اللازمة لها، مما يعني أنه لا حاجة لدولة ما مثلاً، أن تقوم بتصنيع أسلحة مكلفة جداً كحاملات الطائرات والمقاتلات المتطورة، لتشكل تهديداً خطيراً وحقيقياً على دولة كبيرة مثل الولايات المتحدة الأمريكية.
- تمتّع المهاجم بأفضلية واضحة في حروب الإنترنت على المدافع، لأنها حروب تتميز بالسرعة والمرونة والمراوغة، ومن الصعب على عقلية التحصن لوحدها أن تنجح بمواجهة هذه الجرائم، لأن التحصين يجعل المدافع عرضة لمزيد من محاولات الاختراق ومزيداً من الضغط.
- فشل نماذج "الردع" المعروفة، حيث تم تطبيق مفهوم الردع في الحرب الباردة، وهو غير ذي جدوى في حروب الإنترنت، ولا ينطبق عليها، بعكس الحروب التقليدية. كما أن من الصعوبة بمكان أيضاً استخدامه، فقد يكون من المستحيل تحديد الهجمات الإلكترونية ذات الزخم العالي، كما لا يمكن تتبع مصدرها، حتى وإن تم تتبع مصدرها فقد يتبين أنها تعود لفاعلين غير حكوميين، وفي هذه الحالة لن يكون لديهم أصول أو قواعد لكي يتم الرد عليها.
- تتعدى مخاطرها استهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحساسة في البلدان المستهدفة، وقد ظهر واقعياً القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى انفجارات أو دمار هائل(البداينة، 2002، ص217-230).

وأكثر ما يمكن أن تظهر به العلاقة بين الإرهاب الإلكتروني والحرب الإلكترونية تلك المصادر أو الطرق التي يمكن من خلالها الحصول على المعلومات والتي تعد أيضاً من طرق ووسائل تنفيذ الهجمات الإلكترونية سواء في ظل حرب إلكترونية أم في ظل إرهاب إلكتروني وهذه المصادر هي(باكير، 2010، ص2-3):

أولاً: استخبارات المصادر المفتوحة: إذ أن هناك الكثير من المصادر للمعلومات التي تمكن من جمع المعلومات بصورة سهلة ورخيصة ويتم الحصول عليها بسرعة ودون الحاجة لوقت كبير في جمعها وهي قانونية إلا إذا اخترقت الخصوصية وحقوق الإنسان وحقوق الملكية.

ثانياً: المتصفحات وتقنيات الحاسب الآلي: ومن أمثلتها النتسكيب والاكسبلورير، ومنها متصفحات تجعل الدخلاء يتمكنون من الوصول إلى الحاسبات الشخصية، ومعرفة المعلومات الموجودة فيها والمعلومات المدونة على الشبكة عن أي شخص، ومن أمثلة المتصفحات والتقنيات(إبراهيم، 2009، ص39-43):

أ. بروتوكول النص الفائق (HTTP): ويمكن هذا البروتوكول مواقع الإنترنت والمتصفحات من الاتصال وتبادل الوثائق والصور والصوت، وفي بعضها خصائص تمكن من تتبع نشاطات مستخدميها.

ب. تحميل البرمجيات المجانية: وهذه تتطلب معلومات عن الشخص أو أنها قد ترسل لك استبانة إلكترونية تتضمن معلومات هامة دون علمك.

ج. محركات البحث: بعضها يوفر خاصية البحث عن الأفراد، ومن الممكن البحث تحت مواقع البرامج المجانية لتكشف معلوماتك ومنها غوغل وياهو. فهي ممر اجباري لكل باحث عن المعلومات على الانترنت لانها تفهرس ملايين الصفحات وتسمح بالبحث فيها للحصول على نتائج سريعة بدلا من البحث اليدوي على الشبكة.

د. البريد الإلكتروني: ويعمل البريد الإلكتروني على تهديد الخصوصية من خلال الحصول على بعض المعلومات المتعلقة به، ويسهل استخدامه لاحتوائه أسماء أشخاص وتسهيله

لعمليات جمع المعلومات. كما أنه عرضة للاعتراض من خلال برامج معينة تقتحم البريد الإلكتروني للجهات المستهدفة، إلا أنه يمكن الوقاية من ذلك باستخدام برامج التشفير.

ه. بريد القمامة: وهي مواقع تسعى للحصول على عناوين البريد الإلكتروني من خلال إغراقهم بالدعايات التجارية، أو من خلال الاجتماعات والنقاشات في المنتديات.

و. التجارة على الإنترنت: وهذا يتم من خلال استخدام بطاقات ائتمان، إلا أن البعض يرى أنها غير آمنة، ويتم الحصول على المعلومات عن الأشخاص من خلال تقديم العميل اسمه ومعلوماته عندما تطلب منه على الشبكة للقيام بهذه العملية.

ز. التفتيش في القمامة: وهو عمل غير ممنوع من حيث القانون، لكنه غير أخلاقي حيث تقوم مجموعات بالبحث في القمامة للحصول على معلومات تتعلق ببطاقات الائتمان، أو للحصول على الأسرار الصناعية أو للحصول على معلومات شخصية لبيعها.

ح. الشمشمة: وهي برامج لالتقاط الأرقام وكلمات السر الخاصة بالمستخدمين الرسميين، مع وضع برمجيات أخرى تساعدهم على الوصول للبيانات وتدميرها أو الحرمان من استخدامها.

ط. تصفح الويب: وذلك من خلال جمع مشغلات الواقع على الويب للمعلومات عن الزوار والمستخدمين، وعناوين الـ IP للمستخدمين، ونوع النظام، ونوع التصفح، وعدد الصفحات، والوقت وغير ذلك.

ي. استغلال الملكية الفكرية: يصعب حماية هذه الملكيات، إلا أنه غالباً ما تفسر على أنها حقوق طبع ونشر وإنتاج وغيره، وتعد هذه الملكيات أهدافاً صالحة لحرب المعلومات لاستفادة الطرف الآخر منها.

ك. خرق الملكية الفكرية على الإنترنت: والملكية الفكرية على الإنترنت أربعة أنواع: حقوق الطبع، والعلامات التجارية، وبراءات الاختراع، والأسرار التجارية.

ل. طرق حقوق النشر: امتلاك واستخدام أو الادعاء لملكية عمل محمي دون موافقة المؤلف وعند بيع العمل بمقابل مادي لا يتم التعويض المادي المناسب للمؤلف أو صاحب العمل أو الجهة ذات حق النشر.

م. قرصنة البرمجيات: إعادة إنتاج غير قانونية لبرمجيات الحاسب سواء كان ذلك للدعاية أو التجارة أو الاستخدام الشخصي، فتؤدي إلى إفقار جهات مقابل إثراء أخرى لم تبذل أي مجهود فكري أو مادي وقد يؤدي ذلك إلى إفلاسها. وتعد هذه البرمجيات أهدافاً صالحة لحرب المعلومات.

ن. خرق حماية الاتصالات والبيانات: أي التعدي على أو اعتراض أو استخدام أو إساءة استخدام أو الحرمان من خدمة الاتصالات والبيانات وتشمل: التعدي على البيانات وعلى سريتها ووحدة وجودها وحفظها بعيداً عن متناول يد أصحابها، ويشمل هذا التعدي النسخ غير القانوني للبيانات وتحليل المرور الإلكتروني لها، والقنوات المخفية والتعديات على البرمجيات واختطاف الحلقة والإلتفاف وتعديات التوقيت. وخرق الخصوصية: من خلال التنصت ومراقبة سلوك الناس بالعيون الإلكترونية.

س. الكعكات: تعد الكعكات الخصوصية على الإنترنت وهي معلومات يرسلها الموقع على الإنترنت إلى الحاسب الآلي عند اتصاله به ويقوم الحاسب بحفظها عند تلقيها وتعمل على تمكين الموقع من وضع معلم فريد محدد إلى ذلك الحاسب الذي يستخدم ليرتبط مع الطلب المقدم إلى الموقع من ذلك الموقع مسبقاً، ويمكن للكعكات أن تكون عن الشخص صفحة تحتوي على معلومات كاملة عن المستخدم، ويمكن مكافحة الكعكات من خلال وضع ملفات الكعكات على قراءة فقط وذلك حسب المتصفح أو نظام التشغيل وإعداد الحاسب بحيث تحذف الكعكات كل مرة عند بداية تشغيل الحاسب أو استخدام برامج خاصة بالكعكات مثل Cookie cutter أو Crusher.

ومن جانب آخر فإن هناك علاقة تتمثل ببناء جيوش إلكترونية في الإرهاب الإلكتروني، واستناداً إلى المصادر المذكورة اعلاه، فقد أشارت الباحثة مسبقاً إلى امكانية شخص أو مجموعة من الأشخاص المحترفين والمتمرّسين والمزودين بالمتطلبات الأساسية، استهداف بعض القطاعات التي تستهدفها أي حرب إلكترونية، وتحقيق بعض الجوانب التي تحققها الحروب الإلكترونية أيضاً، إلا أن مجال الحرب الإلكترونية يعد أوسع وأكبر من ذلك، كما أن الأضرار الناجمة ستكون أضخم، بسبب القدرات الهائلة اللازمة لذلك، والتي لا تتاح إلا لدول لديها القدرة والقابلية على استثمار مواردها في هذا الإطار، أي بمعنى آخر أنها متطورة تكنولوجياً وتقنياً، ولديها امكانيات باستخدام هذه القدرات في مجال الحرب، لذا نجد أن بعض الدول تنشط في هذا المجال كالصين، وروسيا، والولايات المتّحدة الأمريكية، وفرنسا، وإسرائيل، والهند، والباكستان، وكوريا الشمالية، وإيران، وتعمل هذه الدول على بناء جيوش من الخبراء الذين يشكّلون نواة إلكترونية للدولة. ولعدم وجود قانون يحكم عمل الحرب الإلكترونية في الفضاء الإلكتروني ويحدد إطارها، فان الأعمال التي تتم فيها، تعكس شخصية وصفات النظام الاستخباراتي القائم في ذلك البلد وتوجهاته العامة، ومثال ذلك محاولة الصينيين لاختراق البنتاغون عام (Lee Smith, 2007).

الفصل الثالث

أركان جريمة الإرهاب الإلكتروني وأشكالها

بالنسبة للإرهاب الإلكتروني ودور الإنترنت أو الفضاء الإلكتروني فيه نجد أنه قد يكون الإنترنت وسيلة للإرهاب التقليدي فيصبح اسمه الإرهاب الإلكتروني، وقد يكون محلاً للإرهاب التقليدي فيسمى أيضاً الإرهاب الإلكتروني، بالتالي فإن الإرهاب الإلكتروني إما أن يكون أداة لارتكاب الجريمة أو محلاً لها.

وكما سبق وأن اوضحت الدراسة، هناك العديد من التعريفات للجرائم المعلوماتية التي تفاوتت بين أن يكون الإنترنت والحاسب الآلي هو أداة ارتكاب الجريمة أو محلاً لها سواء أكانت بيانات منطقية (Software) أو مادية (Hardware) أو على شبكات الاتصال (Networks).

وبتناول الصورة الأولى (عندما يكون الفضاء الإلكتروني وسيلة لارتكاب جريمة الإرهاب) فإن ذلك يدخل في إطار الركن المادي والوسيلة أو الأداة الجرمية التي يتم تنفيذ أفعال وعناصر الركن المادي بها. واذا ما اعتبرنا الفضاء الإلكتروني محلاً للجريمة الإرهابية الإلكترونية، فإن ذلك أيضاً يعد من عناصر الركن المادي للجريمة، ويستدعي الحديث عن صور وأفعال الجرائم الإرهابية، إذ أن الإرهاب الإلكتروني يتخذ عدة أشكال من الجرائم قد تستقل بذاتها. ويتم دراسة هذه الصور والأشكال التي تشكل بمفردها أو بمجموعها جريمة الإرهاب الإلكتروني في مبحث مستقل. كما تقوم الباحثة بدراسة عنصر الخطر باعتباره أهم ما يميز جريمة الإرهاب الإلكتروني.

ومن المعروف والمستقر في القوانين والتشريعات والعلوم الجنائية أن لكل جريمة ركنين هما الركن المادي والركن المعنوي، فالركن المادي هو ماديات الجريمة والفعل الذي يبرز عناصر الجريمة ونية ارتكابها الى الوجود فيتحقق الفعل او النشاط الجرمي تاركا وراءه آثاراً او نتائجاً خصها المشرع

بالتجريم، أما الركن المعنوي فهو ما يتعلق بإرادة ونية ارتكاب الجريمة وهو ركن معنوي يكمن في النفس وفي قصد ارتكاب الجريمة. وعليه فإن جريمة الارهاب هي الاخرى تتكون من ركنين مـــادي ومعنـــوي بصرف النظر عما يميزها.

ومن جانب آخر، فإن جريمة الإرهاب الالكتروني وهي بالأصل جريمة ارهابية تتفق مع جريمة الارهاب التقليدي بكافة عناصرها ومميزاتها باستثناء وجود عناصر تقنية او الكترونية او معلوماتية فيها سواء من حيث اعتبارها أداة الجريمة أو محلها، وبالتالي فإنها تتكون من ركن مادي وركـــن معنـــوي، أساسهما تلك الاركان التي تتوافر في جريمة الارهاب التقليدي باستثناء ما يميزها من الجانب الالكتروني.

ومن هنا تقوم الباحثة بمعالجة هذه الاركان من حيث الافتراض المسبق بأن أركان جريمة الارهاب الالكتروني هي ذاتها –بشكل عام– أركان جريمكة الارهاب التقليدي، وتقوم الباحثة بتطبيق الخـــصائص الالكترونية على هذه الاركان، حيث تتميز جريمة الارهاب الالكتروني من حيث كيفية ممارسة النـــشاط الجرمي ومن حيث محل الجريمة وأداتها.

ولكل جريمة –استناداً إلى مبدأ المشروعية– نص يبينها ويوضح أركانها فلا جريمة بدون نـــص. وتقتضي القواعد العامة أن يكون لكل جريمة أركان وهي الركن المادي والركن المعنـــوي. وأن يكـــون الجاني أهلاً لتحمل المسؤولية. وجريمة الإرهاب تعد مثلها مثل سائر الجرائم تنطبق عليها الأحكام العامة من حيث وجود أركانها ومن حيث المسؤولية الجزائية والمساهمة الجرمية. إلا أن هناك أحكاماً خاصـــة تتتعلق بهذه الجريمة أيضاً تميزعها عن غيرها (العازمي، 2007، ص78).

وتجدر الإشارة في هذا الصدد إلى أن غالبية التشريعات تطبق على جريمة الإرهاب الأحكام العامة للجرائم كما هو الحال في قانون العقوبات، وبعض التشريعات يوليها نوعاً من الأهمية الخاصة فيفرد لها تشريعاً خاصاً لمواجهتها. لذا فإن الباحثة تقسم هذا الفصل إلى مباحث ثلاثة كالآتي:

المبحث الاول: الركن المادي في جريمة الإرهاب الإلكتروني

المبحث الثاني: الركن المعنوي في جريمة الإرهاب الإلكتروني والعقاب عليها

المبحث الثالث: صور وأشكال الجرائم الإرهابية في الفضاء الإلكتروني

المبحث الاول: الركن المادي في جريمة الإرهاب الإلكتروني

يتكون الركن المادي في الجرائم العادية من ثلاثة عناصر رئيسية هي السلوك الإجرامي أو الفعل أو النشاط الذي يسلكه الجاني ويحقق به النتيجة الجرمية، ونتيجة جرمية تترتب على هذا السلوك وإتيانه، ومن ثم وجود علاقة سببية بين النشاط أو السلوك الإجرامي وبين النتيجة. وجريمة الإرهاب عامة تتكون أيضاً من ذات العناصر الثلاثة: السلوك الإجرامي، والنتيجة الجرمية، وعلاقة السببية (مصطفى، محمود، 1983، ص264). وتبعاً لذلك فإن جريمة الإرهاب الإلكتروني والتي تتميز بخصائص تجعلها ذات طبيعة منفردة عن الإرهاب التقليدي والجرائم بشكل عام، فإنها تتكون من هذه العناصر الثلاث. وبما أن النتيجة في الجرائم الإرهابية باتت واضحة وتتمثل بـنتيجة مادية وهي التغيير الذي يحدث في العالم الخارجي كأثر للنشاط الإجرامي والذي يصيب أشخاصاً أو أشياءً، والنتيجة القانونية التي تتركز في الاعتداء على المصلحة التي يحميها القانون عن طريق تعطيلها أو انقاصها وإما عن طريق تعريضها للخطر(العازمي، 2007، ص100).

ويعرف السلوك الإجرامي بأنه النشاط المادي الخارجي الذي يصدر عن الجاني ليحقق النتيجة الجرمية التي يعاقب عليها القانون، وهو عنصر ضروري في كل جريمة(المجالي، 2010، ص212).

أما بقاء الجريمة كمجرد فكرة في ذهن الجاني وصرف النظر عنها ولم ينفذها لا تعد نشاطا مجرما يستحق العقاب ، لأن المشرع لا يعاقب على النوايا الآثمة والمقاصد الشريرة ما لم تخرج لحيز الوجود. وبناءً على ذلك فإن المشرع الجنائي لا يتدخل بالعقاب على الأفعال التي تعد من الأعمال التحضيرية ، كإعداد وسائل وأدوات التنفيذ أو خلق جو مناسب لإرتكاب الجريمة، ومثال ذلك فإن إعداد الجاني للسلاح الذي يود إستخدامه في القتل لا يشكل سلوكا إجراميا في القتل إنما هو من الأعمال التحضيرية(راشد، 1974، ص263. وسرور، 1985، ص237). ولكن قد يشكل ذلك جريمة مستقلة بذاتها هي جريمة إحراز سلاح بدون ترخيص، ومع ذلك فإن المشرع قد يرى أحيانا تجريم بعض صور السلوك رغم انها تتجاوز مرحلة التصميم على الجريمة، بإعتبار أن النشاط لذاته يشكل خطرا على مصلحة

يحميها، ومثال ذلك تجريم الإتفاق الجنائي (م1/206) عقوبات أردني، ثم تجريم المؤامرة على أمن الدولة المادة (م107) عقوبات أردني .

إلا أنه ولأهمية النشاط الجرمي وهو ما يميز هذه الجريمة عن غيرها من الجرائم فإن الباحثة تتناوله بالتفصيل، وهذا يتطلب التعريف بما هية النشاط أو السلوك الإجرامي، أي كيف يتم تنفيذ الركن المادي المكون لجريمة الإرهاب الإلكتروني. ومما يميز هذا السلوك الأداة التي يتم ارتكابه بها فهي مختلفة تماماً عن أداة الجريمة في الإرهاب التقليدي، كما أن الكيفية التي يتم من خلالها ممارسة السلوك والنشاط الإجرامي تختلف جملة وتفصيلاً عن آلية ارتكاب ذلك النشاط في الجرائم التقليدية.

لذا فإن الباحثة تتناول هذا المبحث من خلال المطالب الآتية:

المطلب الأول: كيفية ممارسة النشاط الإجرامي في الإرهاب الإلكتروني

المطلب الثاني: أداة الجريمة في الإرهاب الإلكتروني

المطلب الثالث: النتيجة الجرمية وعلاقة السببية في جريمة الإرهاب الإلكتروني

المطلب الأول: كيفية ممارسة النشاط الإجرامي في الإرهاب الإلكتروني

قد يكون السلوك الاجرامي إيجابيا وقد يكون سلبيا، والسلوك الإجرامي هو كل حركة أو مجموعة حركات إرادية من شأنها أن تحدث تغييرا في العالم الخارجي، فالأصل أنه لا يعد من الأفعال الإجرامية تلك الوسائل المستخدمة أو مكان إتيان النشاط الإجرامي أو زمانه، فالجاني يسأل عن القتل المقصود إذا باشر سلوكا إجراميا أدى إلى إزهاق روح غريمه، ولا تعويل عندئذ على الوسيلة المستخدمة أو زمان إرتكاب الفعل أو مكانه ، فكل وسائل القتل لدى المشرع سواء. وقد يأخذ السلوك الإجرامي صورة الإمتناع (النشاط السلبي) فتتحقق الجريمة بالإمتناع من خلال عناصر هي ضرورة الإحجام عن إتيان فعل إيجابي كإنباء السلطة العامة بالجناية المخلة بأمن الدولة، والثاني هو ضرورة الإمتناع من شأنة الإخلال بواجب قانوني والثالث ضرورة توفر الصفة الإرادية للإمتناع ، أي أن تكون الإرادة مصدر الإمتناع(حسني، 1989، ص277).

وقد يتدخل المشرع ويدخل أحد عناصر السلوك في الإعتبار ويعدها من العناصر اللازمة لتحقيق السلوك كإستعمال طرق إحيتالية لقيام جريمة الإحتيال (م417) عقوبات ، وقد تكون وسيلة السلوك مجرد ظرف مشدد للجريمة ، مثل إنتهاك حرمة المنازل عن طريق العنف على الأشخاص أو الكسر وإستعمال السلاح (م2/347) عقوبات ، وقد يعول المشرع على عنصر المكان في بعض الجرائم وإعتباره من عناصر السلوك الإجرامي مثل جرائم الم والقدح والتحقير في مكان علني (المواد 188 و 189) عقوبات، وقد يعد الزمن ظرفا مشددا لعقوبة جريمة ما ، مثل جريمة إنتهاك حرمة المنازل ليلا (م2/347) عقوبات .

أما بالنسبة للفعل أو النشاط الجرمي المكون للركن المادي بالنسبة لجريمة الارهاب التقليدي فإنه يتكون من مجموعة من الافعال كاستعمال ادوات ومواد تشكل خطراً عاماً أو انها تثير الذعر العام أو التهديد باستخدامها او احداث ضرر جسيم من خلالها. ويمكن العثور على هذه الافعال في قانون العقوبات الاردني، ومنه يتضح ان الركن المادي لجريمة الإرهاب التقليدي هو الأفعال المتمثلة باستعمال

الأدوات أو المواد أو الوسائل المذكورة في المادة 147 من قانون العقوبات الاردني، وقد جاءت هذه الوسائل على سبيل المثال لا الحصر، بالتالي فإن كل فعل من شأنه أن يشكل خطراً عاماً وأن يثير الذعر العام، والذعر العام المتجرد من استخدام أي وسيلة من الوسائل ذات الخطر العام. إذ تنص الفقرة الأولى من المادة 147 من قانون العقوبات الأردني على أنه:" يقصد بالإرهاب: استخدام العنف بأي وسيلة كانت أو التهديد باستخدامه....".

ويعد السلوك أو النشاط الإجرامي ذلك النشاط الذي يخالف به صاحبه القاعدة القانونية، ويتم بحركة ايجابية أو سلبية بالامتناع عن اتيان فعل يعد واجباً القيام به تنفيذا لقاعدة قانونية، وذلك لإخراج الركن المادي للجريمة إلى أرض الوجود. بالتالي لا عقاب على النوايا ولا على الأعمال التحضيرية إلا في إطار بعض الجرائم الخطيرة كتلك الماسة بامن الدولة بما فيها الإرهاب(عالية، 1996، ص197).

وبالنسبة للإرهاب نجد أنه من غير المتصور أن تقع جرائمه بالامتناع، إذ أن أغلبها جرائم تتم بأفعال إيجابية والسلوك الايجابي هو السلوك الممكن أن يتم باستخدام الوسائل القادرة على احداث الخطر العام أو الضرر الجسيم. ومن المادة 147 نجد أن العناصر المكونة للسلوك الإرهابي في التشريع الأردني هي استخدام العنف بقصد الترويع أو التهديد أو الرعب (العازمي، 2007، ص97). ولا يصلح التخويف أن يكون عملاً إرهابياً لأنه يتطلب استخدام وسائل تصلح بذاتها لتحقيق عنصر الذعر والتخويف (الجبور، 1993، ص276).

أما بالنسبة للركن المادي في الجرائم الارهابية الالكترونية، فإن الباحثة تشير بداية إلى ان الركن المادي للجريمة المعلوماتية بشكل عام عبارة عن سلوك يتضمن وجود بيئة رقمية وجهاز كمبيوتر وتوافر اتصال بشبكة المعلومات، بالتالي فإنه سلوك يتم من خلال الكمبيوتر أو باستخدام المعالجة الآلية للبيانات(إبراهيم، 2009، ص99-100). ويلزم أن تتم مباشرة النشاط التقني المؤدي إلى الجريمة، ويؤثر ذلك في بناء الأدلة فلا يمكن القول بامكانية توافر الأدلة لاحقاً إذا لم يباشر الشخص النشاط التقني فلا جريمة من هذا القبيل إذا بنيت على مجرد الاعتراف (بن يونس، 2004، ص256).

أما بالنسبة للنشاط الجرمي للارهاب الالكتروني تجد الباحثة تتعدد في صور هذا النشاط، حيث تتوافر جريمة الإرهاب عبر الإنترنت عند استخدام تقنية الإنترنت لبث الافكار الإرهابية، كاللجوء إلى الإنترنت لتحميل صفحات تبين كيفية اعداد القنابل والأسلحة والذخيرة والمواد اللازمة لها وكيفية تركيبها وطرق تنفيذها والمدد الزمنية اللازمة. ولا تقف جريمة الإرهاب عبر الإنترنت عند حدود الجريمة الواحدة أو الوصف الجرمي الواحد، اذ تعد جريمة إرهابية كل جريمة لها أثر في ترويع وتهديد الأمن الداخلي والدولي بما ينجم عن تهديد النظام الوضعي أو النظام العام. وعادة ما تقف جرائم الإرهاب عند حد الشروع لأنها واقعياً لا تصل إلى حد الارتكاب الكامل، وهذا ما يبرر تجريم الأعمال التحضيرية، كحيازة المادة الإرهابية. وتأخذ مسألة حيازة المادة الإرهابية على الإنترنت أبعاداً متغايرة، فهي في العالم الإلكتروني عبارة عن برمجيات (بن يونس، 2004، ص657).

وبالرجوع الى النصوص القانونية في التشريعات الاردنية التي تعالج جانب من الانشطة او الافعال التي قد تعد من جرائم الارهاب الالكتروني او انها تصاحبها او تساعد في تحقيقها نجد أن المشرع الاردني قد جرم الإرسال أو النشر قصداً عن طريق نظام المعلومات أو الشبكة المعلوماتية بيانات أو معلومات أو أنشئ موقعاً إلكترونياً لتسهيل القيام بأعمال إرهابية أو الاتصال بجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو ترويج أفكارها، أو تمويلها، فيعاقب بالأشغال الشاقة المؤقتة (المادة 11 من قانون جرائم انظمة المعلومات الاردني المؤقت). حيث يلاحظ ان النشاط الذي يكون جريمة تسهيل القيام باعمال ارهابية يتمثل في نشاط الكتروني ويتم بوسيلة الكترونية وهو إرسال بيانات أو معلومات أو نشرها قصداً عن طريق نظم المعلومات أو الشبكة المعلوماتية لتسهيل القيام يأعمال إرهابية أو لتسهيل الاتصال بجماعة ارهابية أو بجمعية تقوم بأعمال ارهابية أو تسهيل ترويج أفكارها أو تمويلها. ولو ان المشرع اراد تجريم هذه الافعال بشكل مستقل لوجدنا نصوص –وقد عالجتها الدراسة عند الحديث عن الحماية الجنائية لوسائل الاتصالات– تجرم هذه الافعال وتعاقب عليها بعقوبات لا يزيد حدها الاعلى عن سنتين وليس 15 سنة كما في هذه الجرائم.

ومنها أيضاً جريمة الدخول قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور

تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة ألاف دينار(المادة 12/أ). وإذا كان هذا الدخول بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو بث أفكار تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار(المادة 12/ب).

وتقترب هذه الجريمة من الجرائم الارهابية ويتم الركن المادي لها من خلال نشاط يقوم به الجاني يتمثل بالدخول قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، وذلك بهدف إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو بث أفكار تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، حيث عاقب المشرع على هذه الجريمة بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

وبالنظر إلى النشاط الجرمي الذي تتكون منه هذه الجريمة نجد أنه يتشابه مع بعض الأنشطة الإرهابية في أكثر من جانب، فمن حيث وسيلة ارتكاب النشاط الارهابي، ومن حيث اعتبار الفضاء الالكتروني بيئة للجريمة، ومن حيث تأثيرها ومساسها بمصالح المجتمع العليا وهي الأمن والسكينة خاصة الأمن الوطني لما فيه من تحقيق للمصلحة العامة. إلا أنه لا يمكن اعتبار تجريم هذا الفعل كافيا لتغطية باقي الانشطة الاجرامية التي ترتبط بالارهاب وتتم من خلال وسائل الكترونية.

وهناك وسائل عامة تستخدم في جميع أشكال الإرهاب الإلكتروني أي ما يكون منها إرهاباً بشكل عام ووسائل على المستوى الدولي أو الإرهاب الدولي الإلكتروني، وهو صنف من صنوف الحرب

الإلكترونية أو حرب المعلومات التي تم بحثها في الفصل السابق. لذا فإن الباحثة تتناول هذه الوسائل فيما يتعلق بكيفية تنفيذ الإرهاب الإلكتروني بشكل عام في فرع، وتلك الوسائل على المستوى الدولي في فرع ثان.

الفرع الاول: الأساليب العامة للإرهاب الإلكتروني

ويمكن ايجاز كيفية تنفيذ الإرهاب الإلكتروني وخطوات السلوك الإجرامي كالآتي، علماً بأن هذه الخطوات يعاقب عليها في القانون، وإن كانت في مراحلها الأولى أو في المرحلة التحضيرية للجريمة[5]:

أولاً: مرحلة التحضير والبناء

حيث تمر العملية الإرهابية بمرحلة البناء والحضانة، من خلال تجنيد أعضاء المجموعة الإرهابية، وتدريبهم وتعريفهم بمبادئ المجموعة، والبحث عن التمويل المناسب واللازم لضمان استمرارية الجماعة في عملها، وتجهيز أعضائها وتزويدهم بكافة الأدوات التي تلزم تنفيذ جرائمهم كوسائل الاتصال والنقل والتخفي والتدريب وتقسيم العمل والمهام. وفي هذا الصدد تجدر الإشارة إلى أن وسائل التكنولوجيا والاتصالات الحديثة قد قللت من تأثير المسافات والأزمنة اللازمة لارتكاب الجريمة والتي قد تعيق انتقال الأفكار والمعلومات والأشخاص، ومن هذه الوسائل الهواتف الثابتة والنقالة والإذاعة والتلفزيون (نظمي، 2010، ص14).

وتتميز هذه المرحلة بالتلقين الإلكتروني من خلال قيام الإرهابيين بحشد المؤيدين والمتعاطفين معهم، خاصة من فئة الشباب[6]، وبث مبادئهم وطرقهم ووسائلهم في محاولة لتجنيد إرهابيين جدد. فهناك

---

5 لا يعني ذلك ترتيب هذه الخطوات، ولا يعني اشتراط القيام بها في كل الجرائم الإلكترونية، فقد تحدث في جرائم دون أخرى، وبعض الجرائم قد تتم بها كل هذه الخطوات وبعضها ربما خطوةً واحدةً منها أو ربما أكثر من خطوة.

6 يتم تجنيد الشباب من خلال بعض المظاهر والأساليب كالاتي (نظمي، 2010، ص20):

1- الدعوة إلى القيام ببعض الاعمال، والدعوة إلى إنكار مظاهر الفساد وتحلل المجتمع، لتحرير وايقاظ دوافع اعتراض الناس على تشكيل اتجاهات متطرفة.

2- الدعوة الحماسية من خلال تحفيز وتشجيع المخالفين وإرسال المنشورات والخطب التكفيرية.

3- الدعوة إلى القيام بأعمال سامية، مثل الدعوة إلى إحياء فريضة الجهاد الغائبة.

4- عقد الاجتماعات مع الأشخاص الراغبين من خلال غرف الدردشة والمنتديات.

5- تكذيب قصص وروايات الشباب المعارضين للمشاريع الإرهابية والشباب الذين ظهروا نادمين لانخراطهم في بعض أعمال التفجير والعنف.

آلاف المواقع للمنظمات الإرهابية لنشر أفكارها ومعتقداتها والتخطيط والتجهيز للعمليات الإرهابية المنوي القيام بها، وتنسيق وتبادل الخبرات الميدانية العملية بين الإرهابيين، حيث تم الكشف عن مواقـــع لتعلـــيم صناعة المتفجرات والألغام والأسلحة الكيماوية الفتاكة، ومواقع توضح آلية اختـــراق وتـــدمير المواقـــع والبيانات والنظم المعلوماتية واختراق البريد الإلكتروني، وكيفية الدخول إلى المواقع المحجوبة، وعمليات التجسس الإلكتروني، وطرق نشر الفيروسات. كما أن هناك مواقع مخصصة لشن حملات نفـــسية علـــى الدول والمجتمعات التي تقوم بترويعها، حيث تعرض الرهائن والأسرى وكيفية إعدامهم.

ثانياً: اقتحام المواقع الإلكترونية وتدميرها

أي الدخول إلى المواقع الإلكترونية وتدميرها وتغيير محتوياتها والدخول إلى الشبكات والعبـــث بمحتوياتها بازالتها أو بالاستيلاء عليها أو الدخول على شبكات الطاقة أو شـــبكات الاتـــصالات بهـــدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً. ولتدمير المواقع يتم الدخول غير المشروع إلـــى نقطة ارتباط أساسية، أو فرعية متصلة بالإنترنت من خلال نظام آلي (Server–PC)، أو مجموعة نظم مترابطة شبكياً (Intranet)، بهدف تخريب نقطة الاتصال أو النظام (داود، 2000، ص83. والجنبيهـــي منير والجنبيهي ممدوح، 2005، ص111).

ويعد النظام الإلكتروني بيئة سهلة للاختراق، والحيلولة دون الاختراق تعد من المسائل الصعبة، اذ ليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم، بسبب المتغيرات التقنية الدائمة، وإلمام المخترقين – أي مرتكبي جرائم الاختراق– بثغرات الإنترنت وتطبيقاته والتي تقوم على أساس التصميم المفتوح لمعظم الأجزاء، سواء أكان ذلك في مكونات نقطة الاتصال، أو النظم، أو الشبكة، أو البرمجة.

وتعد المواقع الإلكترونية في كثير من الأحيان هدفاً للجماعات الإرهابية لكي تقوم بتدميرها واتلاف محتوياتها، خاصة وأن الجماعات والتنظيمات تمتلك من الوسائل التي تسهل الاختراق ما لا يمتلكه الافراد العاديين. ويستفيد المخترقون من عمليات الاختراق هذه في الوصول إلى كثير من المعلومات الخاصة

والأسرار الشخصية واختراق الخصوصية. كما يعد ذلك أمراً سهلاً عليهم، إذ نجد في مجرمي الحاسب الالي والإنترنت المهارة العالية في تحقيق أهدافهم وارتكاب جرائمهم وأنهم من الاذكياء والمحترفين والخبراء. ويمكن أن تتم عملية الاختراق من أي مكان في العالم طالما كان هناك أجهزة حاسب آلي متصلة بالإنترنت، بالتالي تستفيد الجماعات الإرهابية من هذه الميزة وتقلل من مصاعب الأبعاد الجغرافية، إذ يمكن للمجرم المعلوماتي ارتكاب هذه الجريمة من أي مكان في العالم ضد أي جهاز متصل بالشبكة في أي مكان من العالم أيضاً.

تجدر الإشارة في هذا الصدد أن عمليات الاختراق والولوج عادة تتم من قبل مجموعات محترفة تعرف طرق التخفي والتلاعب بالبيانات الشخصية لها، لأن مزود الخدمة قد يعرف حركة المشترك بمجرد اتصاله بالشبكة ويعرف كافة بياناته وتفصيلاته الشخصية وكل ما يقوم به من أنشطه على الشبكة من خلال الرقم الخاص (IP)، حتى أن باستطاعته أن يكتشف المواقع التي زارها، والكلمات التي بحث عنها، والصفحات التي اطلع عليها وما جلب منها من ملفات، والتاريخ، وما قام به من حوارات، كما يستطيع معرفة الرسائل الإلكترونية التي تم تبادلها، وعمليات الشراء وتفصيلاتها(السند، 2005، ص24).

وبالرغم من أن الواقع العملي يزيد من صعوبة ذلك، بسبب كثرة المعلومات والأنشطة التي يقوم بها الافراد إذ تحتاج هذه العمليات لجهود مضنية وطويلة، لكن يبقى الأساس النظري هو إمكانية ذلك. وهذا ينفي اعتقاد البعض أن مجرد الدخول باسم وهمي سوف يحقق ميزة التخفي (عبدالمطلب، 2000، ص42). لذا نجد أن مرتكبي الجرائم يمتلكون من الذكاء والطرق والأساليب المبتكرة للتخفي للقيام بعمليات الاختراق دون أن يتركوا أثراً خلفهم.

وهناك عدة طرق للاختراق وتدمير المواقع، منها:

1. الإغراق بالرسائل: وهي ربما تكون طرق مستقلة بذاتها لتنفيذ السلوك الإجرامي في جرائم الإنترنت ويمكن بحثها بشكل مستقل في هذا المجال، إلا أن الباحثة تكتفي في هذا الجانب بالإشارة اليها.
2. التلاعب بالبيانات: وتقوم هذه الجرائم أساساً على التلاعب بالبيانات والمعلومات والبرامج من

خلال المعالجة الآلية للبيانات لمحوها أو تعديلها أو تشويهها أو إلغائها أو تحويل مجراها، وتتمثل الصورة الغالبة في تحقيق غاية المجرم المعلوماتي في نطاق شبكة الإنترنت من خلال الدخول غير المشروع إلى النظام المعلوماتي، أو البقاء فيه دون إذن، ثم قيام الجاني بارتكاب فعله، والذي قد يكون مجرماً بنصوص عقابية أو غير مجرم (الشوابكة، محمد، 2004، ص1)[7].

والإرهاب بحكم أنه واحداً من صور جرائم المعلوماتية فإنه يتم ارتكابه بذات الطريقة إذ أن الإرهابي المعلوماتي (المجرم المعلوماتي) يقوم بالدخول غير المشروع إلى النظام أو البقاء فيه بدون إذن ثم يقوم بمباشرة أفعاله بالتالي من الضرورة بمكان الحديث أولاً عن آلية ارتكاب الإرهاب الإلكتروني قبل التطرق إلى صوره ومظاهره ووسائله. علماً بأن الدخول غير المشروع إلى النظام أو البقاء فيه يعد بذاته فعلاً مجرماً، وسنتناول هذه الجريمة بشكل مستقل في المبحث الثالث من هذه الدراسة وعن موقف المشرع الأردني باعتبارها صورة من صور الجرائم الإرهابية.

3. تدمير أنظمة المعلومات: يعرف تدمير أنظمة المعلومات بأنه محاولة اختراق شبكة المعلومات الخاصة بالأفراد أو الشركات بهدف تخريب نقطة الاتصال أو النظام عن طريق تخليق أنواع من الفيروسات الجديدة التي تسبب كثيراً من الضرر والشلل لأجهزة الكمبيوتر والمعلومات التي تم تخزينها على هذه الأجهزة، ومثال ذلك في أستراليا عام 2005 حيث تمكنت منظمات إرهابية من تدمير شبكة الصرف الصحي في إحدى المدن مما نجم عنها أضرار صحية واقتصادية فادحة (المصري، 2011، بدون رقم صفحة).

وهناك أسباباً تسهل عمليات تدمير المواقع تتمثل بالاتي(السند، 2005، ص24–25):

أ. ضعف الكلمات السرية، مقابل وجود طرق ذكية لدى المخترقين لامكانية توقعها ومعرفتها.

---

7 . ويعرف النظام المعلوماتي انه:"النظام الذي يستخدم لإنشاء رسائل بيانات أو ارسالها أو استلامها أو تخزينها أو لتجهيزها على اي وجه آخر"(ابراهيم، 2009، ط1، ص23).

ب. عدم استخدام ووضع برامج الحماية اللازمة، لمنع الاختراقات وتدمير المواقع. أو عدم القيام بالتحديث اللازم لها(update)، إذ أن هذه المواقع تعمل على تنبيه المستخدم لأية محاولات اختراق لجهازه على الشبكة.

ج. قد يكون الضعف والخلل من قبل مزودي الخدمة، فبعض الشركات لا تكون قادرة على تأمين الدعم الفني المستمر للمشتركين، أو أنها قد تستخدم برامج وأنظمة ضعيفة وغير موثوقة ولا يجري العمل على تحديثها.

د. عدم التحديث المستمر لأنظمة التشغيل، فقد يتبين مع الوقت بعض الثغرات الأمنية بها، الأمر الذي يستدعي تحديثها لعلاج هذه الثغرات.

وهناك عمليات تخزين احتياطية تسمى بالانجليزية الــ (Backup)، وإن عدم القيام بهذه العمليات يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها.

ثالثاً: إنتحال شخصية الفرد

ساهم انتشار الإنترنت باعطاء المجرمين قدرة أكبر على ارتكاب جرائم انتحال الشخصية وذلك من خلال المساعدة في عمليات جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم، وتتم هذه الجريمة من خلال عدة وسائل وصور منها الاعلانات المشبوهة والتي منها ما يداعب غريزة الطمع الانساني، للعمل على الاستيلاء على معلومات اختيارية من الضحية، مثل الاعلان عن جائزة ضخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، وتتطلب هذه العملية الافصاح عن بعض المعلومات الشخصية كاسم االضحية وعنوانها ورقم بطاقة الائتمان. ويظهر من خلال ذلك إمكانية ارتكاب جرائم أخرى نتيجة لهذه الجريمة كجريمة الاستيلاء على رصيد بنكي أو السحب من بطاقته الائتمانية أو حتى الاساءة إلى سمعة الضحية (الجنبيهي منير والجنبيهي ممدوح، 2005، ص42).

رابعاً: انتحال شخصية المواقع

يعد هذا الأسلوب من الأساليب الحديثة نسبياً ويتمتع بخطورة واضحة لصعوبة اكتشافه، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع ذات نظم الاتصال الآمن (Secured Server)، ويمكن وبسهولة اختراق الحاجز الأمني من خلال هجوم المجرم على الموقع للسيطرة عليه، ثم تحويله كموقع بيني، أو من خلال اختراق موقع أحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك، مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور (داود، 2000، ص89-93. والجنبيهي منير والجنبيهي ممدوح، 2005، ص45).

خامساً: الإغراق بالرسائل

ويتم ذلك من خلال ضخ مئات الآلاف من الرسائل الإلكترونية إلى الموقع المستهدف، حيث يؤثر ذلك في السعة التخزينية للموقع، وتشكل ضغطاً كبيراً عليه، قد يؤدي بالنتيجة إلى اضعاف الموقع ثم تفجيره، وتشتيت البيانات والمعلومات المخزنة فيه وانتقالها إلى جهاز المرسل. كما يمّكن ذلك المرسل من التجول داخل الموقع المستهدف بسهولة ويسر وامكانية الحصول على البيانات والمعلومات الخاصة والمستهدفة (الخليل، 2000، ص4).

كما يؤدي الإغراق إلى تعطل الشبكة وعدم إمكانية استقبال أي رسائل، ويتسبب أيضاً بإنقطاع الخدمة، خاصة إذا كانت الجهة المتضررة من ذلك هي جهة تقديم خدمة الإنترنت. ويتم ذلك من خلال ملء منافذ الاتصال (Communication-Ports) وقوائم الانتظار (Queues) ، الأمر الذي يتسبب بانقطاع الخدمة، وتكبد خسائر مادية ومعنوية غير محدودة، ولمكافحة ذلك لجأت الشركات إلى تطوير برامج تسمح باستقبال جزء محدود من الرسائل في حالة تدفق اعداد كبيرة منها (الجنبيهي منير والجنبيهي ممدوح، 2005، ص67).

ويسمى الإغراق أيضاً بالقصف الإلكتروني، وهو من أساليب الهجوم على شبكة المعلومات، وتلجأ المنظمات الإرهابية إلى تدمير البنى التحتية الخاصة بأنظمة المعلومات في مختلف المواقع. ومثال ذلك تعرض موقع شركة أمازون لبيع الكتب على الإنترنت وشركة سي أن إن الإخبارية للقصف الإلكتروني، مما أدى إلى بطء تدفق المعلومات (المصري، 2011، بدون رقم صفحة)

سادساً: الاقتحام أو التسلل

ويتم التسلل من خلال حصان طروادة الذي تم بيانه، وبعد الدخول يتم التجسس على أعمال الشخص التي يقوم بها على جهاز الحاسب الالي الشخصي لديه فيقوم بتسجيل كل حركاته وأعماله من أول طرقة يقوم بها على لوحة المفاتيح منذ أول لحظة للتشغيل، ويشمل ذلك أيضاً الحصول على البيانات السرية والحسابات المالية والمحادثات التي يجريها على الشبكة وأرقام بطاقات الائتمان الخاصة به وكلمات المرور، ثم يتم إستخدام هذه المعلومات من قبل الجاسوس المتسلل . ويعد هذا الفعل مجرماً ومن الجرائم الشائعة في العالم(الجنبيهي منير والجنبيهي ممدوح، 2005، ص46-47).

ويستخدم المجرمون أيضاً هذا الفعل أو هذه الطريقة لارتكاب جرائم أخرى ومنها الإرهاب والجرائم المنظمة، وقد اكدت المباحث السرية الامريكية(The US Secret Service) أن عصابات الجرائم المنظمة تتجه نحو استغلال التسلل (Hacking) للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية. ويتم التسلل من خلال زرع حصان طروادة في جهاز الضحية بعدة طرق منها(الجنبيهي منير والجنبيهي ممدوح، 2005، ص58):

1. عن طريق البريد الإلكتروني كملف ملحق، حيث يقوم الشخص بإستقباله وتشغيله، وقد يرسل ضمن برامج أو ملفات أخرى.
2. من خلال برنامج (ICQ) وهو برنامج محادثة انتجته اسرائيل يختصر جملة I seek you

3. عـــند تحميل بـــرامج من أحد المواقع غير الموثوق بها مجرد كتابة كوده على الجهاز نفسه في دقائق معدودة
4. من خلال اتصال الجهاز بشبكة داخـــلية أو شبكة إنترانت
5. من خلال برنامج(FTP) أو (Telnet)الخاصة بنقل الملفات
6. من خلال بعض البرامج الموجودة على الحاسب مثل الماكروز الموجود في برامج معالجة النصوص

وتتم عملية الإختراق، من خلال اعتماد برامج القرصنة بشكل كلي على بروتوكول(TCP/IP)، وهناك أدوات تعرف بـــ (ActiveX) مصممة وجاهزة لخدمة التعامل بهذا البروتوكول ومن أشهرها (WINSOCK.OCX) الخاص بمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الأدوات، ويحتاج الاختراق إلى برنامجين هما: خادم في جهاز الضحية، وعميل في جهاز المتسلل، حيث يقوم الخادم بفتح منفذ في جهاز الضحية، ويكون هذا المنفذ معروف من قبل العميل أصلاً، أما برنامج الخادم فيكون في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية، حيث يتعرف برنامج الخادم (server) على إشارات البرنامج المخترق، ويتم الاتصال، ومن ثم يتم عرض محتويات جهاز الضحية كاملة لدى المخترق، حيث يتمكن من العبث بها أو الاستيلاء على ما يريد منها. والمنافذ أو ما يسمى بالبورتات (Ports)يمكن وصفها ببوابات للجهاز، وهناك عدد من المنافذ في كل جهاز، ولكل منها غرض محدد، فمثلا المنفذ 8080 يكون مخصص لمزود الخدمة، وهو منفذ غير مادي ويعتبر جزء من الذاكرة له عنوان معين، يتعرف عليه الجهاز بأنه منطقة يتم إرسال واستقبال البيانات عليها، ويمكن إستخدام عدد كبير من المنافذ للإتصال وهناك ما يقارب الـــ (65000) منفذ تقريباً، ويتميز كل منفذ عن الآخر برقم خاص، وما يقوم به المتسلل عبارة عن فتح أحد هذه المنافذ فقط حتى يستطيع الوصول لجهاز الضحية، وهوما يسمى بطريقة الزبون/ الخادم (Client\Server)، حيث يتم ارسال ملف لجهاز الضحية يفتح المنافذ، فيصبح جهاز الضحية (server) وجهاز المتسلل (Client) مفتوحاً، ثم يقوم المستلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج (NetBus) أو (NetSphere) ، وهناك خطورة إضافية عند

دخول المتسلل إلى جهاز الضحية، فهو لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز، حيث يصبح ذلك الجهاز مركزاً عاماً يمكن لأي شخص الدخول عليه بمجرد مسح المنافذ (Portscanning) عن طريق أحد البرامج المتخصصة في ذلك(الخليل، 2000، ص6).

سابعاً: التهديد الإلكتروني

التهديد أساساً عبارة عن أقوال وهذه الأقوال، لا تعد جريمة مالم تخرج إلى العالم المادي، وفي الجرائم الإرهابية يجب توافر عنصر الترويع والتخويف والازعاج لثبوت المسؤولية الجزائية، ومن هنا يأتي الربط بين الإرهاب وكثير من الجرائم التي قد تعد قائمة بحد ذاتها، كالتخريب والاتلاف والقتل، والإرهاب عبر الإنترنت (Dorothy E Dening،2000 ، ، من: بن يونس، 2004، ص649).

ويتخذ التهديد عبر الإنترنت عدة أشكال وصور سواء التهديد بالقتل لشخصيات سياسية أو التهديد بالقيام بتفجيرات في مراكز سياسية أو تجمعات رياضية أو التهديد بإطلاق فيروسات لإتلاف الأنظمة المعلوماتية في العالم. ومن أمثلة التهديد الإلكتروني تهديد شاب أمريكي يدعى "جاهابر جويل" كان يبلغ 18 عاماً حيث هدد كل من مدير شركة مايكروسوفت، والمدير التنفيذي لشركة M.P.I بنسف شركتيهما إذا لم يتم دفع خمسة ملايين دولار، ولدى تفتيش منزله والقبض عليه تم العثور في حاسبه الآلي على عدة ملفات رقمية تحتوي معلومات عن تصنيع القنابل قام بإنزالها عبر الإنترنت وتجميعها (المصري، 2011، بدون رقم صفحة).

الفرع الثاني: وسائل الإرهاب الدولي الإلكتروني

وهي وسائل تبين كيفية ممارسة الإرهاب الإلكتروني على المستوى الدولي، وتأتي إلى جانب بعض أو كل الأساليب العامة في ممارسة الإرهاب الإلكتروني التي تم بيانها في الفرع السابق. وتتمثل

أساليب الإرهاب الإلكتروني على المستوى الدولي (حرب المعلومات أو الحرب الإلكترونية) ببناء الجيوش الإلكترونية والتي تمر بالخطوات الآتية:

أولاً: تطوير الاستعدادات الهجومية

حيث تعد الصين وروسيا الأبرز في هذا المجال، إذ تهتم الصين وتعمل على تطوير قدراتها الهجومية في المجال الإلكتروني، وتدمج مفهوم الثورة في الشؤون العسكرية في عقيدتها العسكرية، خاصة في مجال الحروب الإلكترونية، وتؤكد الورقة الصينية البيضاء عن "الدفاع القومي" للعام 2006 أن الهدف الرئيسي من بناء جيش حديث، هو جعله قادراً على الفوز في حروب المعلوماتية بحلول منتصف القرن الواحد والعشرين. وقد أعادت الورقة البيضاء للعام 2009 التأكيد على ذلك(Elinor Sloan، 2010 ، p: 8، من: باكير، 2010، ص3).

ثانياً: تطوير الاستعدادات الدفاعية

إن الدول الأكثر اعتماداً على الإنترنت تعد الأكثر عرضة لهجمات الحروب الإلكترونية، ولأن الأفضلية كما أشارت الباحثة، في حروب الإنترنت للمهاجم، ولأن ميدان حرب الإنترنت عبارة عن ميدان لا تناظري، فإن الدول تعمل على تطوير قدراتها الدفاعية إلى جانب امتلاكها قدرات هجومية متطورة، ومن هذه الدول انكلترا التي قامت على سبيل المثال بإصدار إستراتيجية الأمن الإلكتروني القومية في حزيران 2009، وبإنشاء وحدة الأمن الإلكتروني، ومركز العمليات الذي يقع مقره في وكالة الاستخبارات القومية (GCHQ)، والتي بدأت وظيفتها عملياً في شهر آذار 2010 (Cyber Security Strategy of the United Kingdom، 2009).

وكذلك الحال بالنسبة لدول حلف شمال الأطلسي أو الناتو، الذي يعتبر الهجمات الإلكترونية بمثابة إعلان حرب أو شكل من أشكال الاعتداء العسكري الذي يفرض على الدول الأعضاء الالتزام بتقديم المساعدة والدفاع عن الحليف الذي يتعرض لهجوم. والولايات المتحدة كذلك والتي تعد الدولة الأكثر

امتلاكاً للقدرات والتقنيات الهجومية العالية المطلوبة في الحروب الإلكترونية، وتهتم أكثر بالجانب الدفاعي لأنها الأكثر اعتماداً على الإنترنت في مختلف القطاعات المدنية والعسكرية، ففي أيار 2009، صادق البيت الأبيض على وثيقة "مراجعة سياسة الفضاء الإلكتروني" التي قدمت من قبل لجنة خاصة إلى الرئيس الأمريكي أوباما، لخصت الخطوات التي يجب على الولايات المتحدة اتباعها لتفعيل الأمن الإلكتروني ومتطلباته الأولية الأساسية (Space Policy Review Cyber).

كما كشفت وكالة الاستخبارات المركزية الأمريكية (CIA) عن مبادرة جديدة لمحاربة الهجمات الإلكترونية (باكير، 2010، ص4). كما قامت في أيار 2010 بإنشاء قيادة الإنترنت "سايبركوم" وعينت مدير وكالة الاستخبارات القومية الجنرال كيث أليكساندر قائداً عليها، تلخصت مهمتها في الحرص على حماية الشبكات العسكرية الأمريكية على الدوام، وقد بدأت هذه القيادة العمل فعلاً في العام 2010 وتضم هذه القيادة ما يقارب 1000 فرد من نخبة القراصنة والجواسيس الإلكترونيين المحترفين والمميزين يعملون تحت إمرة الجنرال أليكساندر(Pentagon may apply preemptive warfare policy to the Internet،2010).

ثالثاً: التجسس الإلكتروني

ويستهدف التجسس الإلكتروني البحث عن أسرار عسكرية ونظم دفاعية عسكرية ومعلومات سرية وتقنيات، وتكمن خطورته في زيادة التنافسية الدولية وعولمة الاقتصاد واعتماد الشؤون العسكرية الاقتصادية وفرص العمل على هذه الاسس كما أنها تضمن التفوق الاقتصادي والعسكري للدول خاصة الصناعية، بالتالي فإن التجسس التقني والاقتصادي هو استثمار غير شرعي لهذا التفوق (الشوا، 1994، ص212). ومن أهم الأشياء المستهدفة في جرائم التجسس والإرهاب الإلكتروني هي(الألفي، 2005،

بدون رقم صفحة. وسلامه، 2006، ص150. والجنبيهي منير والجنبيهـــي ممـــدوح، 2005، ص108-109):

1. المعلومات: حيث يشمل ذلك سرقة أو تغيير أو حذف المعلومات، وفي العصر الحالي عصر المعلومات والتقنية العالية فإن حدود الدولة أصبحت مستباحة بسبب أقمار التجسس والبث الفضائي، كما تحولت وسائل التجسس من الطرق التقليدية الي الطرق الإلكترونية في ظل استخدام الإنترنت وانتشاره.
2. الأجهزة: ويتمثل ذلك بتعطيلها أو تخريبها
3. الأشخاص أو الجهات: حيث تستهدف هذه الجرائم فئة كبيرة من الأشخاص أو الجهات بشكل مباشر كالتهديد والابتزاز. وفي هذا الصدد نجد أن الخطر لا يقتصر فقط على محاولة اختراق الشبكات والمواقع من قبل العابثين من مخترقي الأنظمة HACKERS لأن مخاطرهم محدودة نسبياً وتقتصر غالباً على العبث أو اتلاف المحتويات، وهذا ما يمكن التغلب عليه من خلال ايجاد نسخة احتياطية مخزنة. لكن يكمن الخطر الحقيقي في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية في مختلف دول العالم، للحصول علي أسرار ومعلومات عن غيرها من الدول، وإفشاؤها لدولة أخرى معادية، أو استغلالها بما يضر مصلحة تلك الدولة .

ويتم التجسس بكافة أنواعه للحصول على معلومات وأغلب هذه المعلومات تتم بوسائل اتصال عن طريق الفضاء من خلال موجات لاسلكية ووسائل الاتصال التي تهدف الحصول على المعلومات فـــي أي شكل من أشكال الحرب والإرهاب، وهذه الوسائل هي: التلفون وخدمات الهـــاتف. والتلفـــون الجـــوال. وتسجيل المكالمات. والفاكس. والتلفون اللاسلكي. والبريد الصوتي وآلة الـــرد الـــصوتي. واعتـــراض الاستخبارات الأجنبية. وتحليل رموز الرسائل. والإرســـال بالـــستلايت. والتنـــصت علـــى المكالمـــات الهاتفية(سلامه، 2006، ص147-149).

والتجسس بشكل عام هو استقصاء وسرقة المعلومات الماسة بأمن الدولة من الأفراد أو المؤسسات أو الدول أو المنظمات، بهدف الحصول على معلومات أياً كان نوعها اقتصادية أو سياسية اوعسكرية أو

شخصية. ومثال ذلك في فرنسا في صيف 1994 سعت إحدى الجهات الإرهابية للحصول على المعلومات العسكرية المخزنة في ذاكرة الحاسبات الآلية التابعة لسلاح البحرية الفرنسية وسرقت معلومات عسكرية منها تتعلق بالسفن التي تستعملها الجيوش التابعة لدول أعضاء حلف شمال الأطلنطي الأمر الذي دفع قيادة أركان الحلف والسلطات العسكرية الفرنسية إلى تصميم برامج جديدة لحماية حاسباتها الآلية.

وتعد الشبكة الإلكترونية (الإنترنت) هدفاً للتجسس لاحتوائه على كثير من المعلومات الهامة–وليس كل المعلومات المتوافرة على الشبكة هامة–، حيث ينطبق عليها كشبكة معلوماتية النموذج المعروف لها من المعلومات ذو الأبعاد الثلاثة وهي (الألفي، 2005، بدون رقم صفحة):

أ. سرية المعلومات: ويعني ذلك ضمان حفظ المعلومات المخزنة في أجهزة الحاسب الالي أو الأجهزة المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين لذلك.

ب. سلامة المعلومات: ويتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين لذلك.

ج. وجود المعلومات: وذلك يتمثل في عدم حذف المعلومات المخزنة علي أجهزة الحاسب إلا من قبل الأشخاص المخولين لذلك. بيد أن جرائم الإنترنت ليست محصورة في هذا النموذج بل ظهرت جرائم لها صور أخري متعددة تختلف باختلاف الهدف المباشر في الجريمة.

رابعاً: التنكر والخفاء

تتم حرب المعلومات من قبل المتنكرين والمختفين فهم من يرتكب جرائم الكمبيوتر والإنترنت خلسة وبكافة أشكالها وهم في حالة تنكر وخفاء، لذا لابد من التطرق لبعض أشكال التنكر والخفاء والتي تمثل جرائم من هذا القبيل وضمن ما يتصل بنطاق دراستنا إذ لن نتناول سرقة البطاقات والهويات وأخذ القروض والبطاقات الائتمانية وتزوير السندات والرسائل الإلكترونية والتزوير والتزييف وإن كان يمكن أن ترتكب مثل هذه الأفعال في معرض ارتكاب جرائم الإرهاب من خلال العالم الإلكتروني.

ومن المسائل الهامة في هذا الصدد استخدام برامج حصان طروادة الفيروسية، حيث تستخدم قصة حصان طروادة كرمز للخفاء لأن القصة التاريخية تقول أن الجنود اختبئوا داخل حصان خشبي لفتح البوابة والدخول إلى الحصن وهزيمة الأعداء.

بالتالي فإنه بربط ذلك يتبين أن هناك فيروسات تزرع في جهاز الخصم للدخول إليه وحذف الملفات الموجودة به وإعادة تجهيز القرص الصلب وتحول حصن طروادة إلى قنبلة منطقية أو قنبلة وقت (البداينة، 2002، ص305). وأن هناك وسائل لتدمير أجهزة الآخرين وإتلاف المعلومات عليها وهي: حصان طروادة، والفيروسات وهي أنواع منها ما يتعلق بقطاع التشغيل ومنها فيروسات الماكرو والفيروسات الطفيلية أو فيروسات التنفيذ ومنها فيروسات البرامج، والقنابل المنطقية: وهي مجموعة من تعليمات الكمبيوتر التي تنفذ عملاً مؤذياً عند توفر شروط معينة، وديدان الإنترنت (داود، 2000، ص135).

خامساً: العمليات النفسية التي تتم بالمعلوماتية

وهذه العمليات تعد من المسائل الهامة والأساسية في الحرب الإلكترونية والإرهاب الإلكتروني وهي(البداينة، 2002، ص149)

أ. عمليات نفسية استراتيجية وهي عمليات معلوماتية دولية تقوم بها الدولة للتأثير على اتجاهات الخصم وإدراكاته وسلوكياته باتجاهات محببة لتلك الدولة وأهدافها، عادة ما تتم هذه العمليات خارج الدولة وخارج النطاق العسكري.

ب. العمليات النفسية العملياتية وهي التي تتم قبل الحرب وخلالها وأيام الصراعات وقد تكون موجهة لبقعة جغرافية معينة أثناء الصراعات المفتوحة.

ج. العمليات النفسية التكتيكية وهي التي تنفذ في منطقة لقائد تكتيكي خلال الصراعات أو الحرب لدعم هدف تكتيكي ضد الخصم.

د. العمليات النفسية التماسكية: وهي العمليات التي تنفذ في المناطق الأجنبية العدائية والتي تكـــون ممثلة من طرف الدولة ويوجد فيها خصم أو جماعات عدائية للدولة وتنفذ لإنتاج سلوكيات مؤيدة وداعمة لأهداف الدولة.

المطلب الثاني: أداة الجريمة في الإرهاب الإلكتروني

أشارت الباحثة للتو أن جريمة الإرهاب الإلكتروني تتميز بالأداة الجرمية التي تتم من خلالهـــا، وكإشارة أولية بسيطة فإن جرائم الإرهاب الإلكتروني هي تلك الجرائم التي ترتكب من خـــلال الفـــضاء الإلكتروني أو الإنترنت، فيكون الإنترنت أو الشبكة الإلكترونية أو الكيان المنطقي، وتطبيقات هذه الشبكة، إلى جانب الممارسات والعمليات التي يمكن أن تمارس من خلال الإنترنت، هي الأداة الجرمية في جريمة الإرهاب الإلكتروني، وذلك بخلاف الجرائم التقليدية التي تتميز أداتها –إن ارتكبت من خلال أداة– بأنهـــا أدوات تقليدية كالمتفجرات والأسلحة والذخائر وغيرها. وستتضح هذه البدايات تباعاً مـــن خـــلال هـــذه الوسائل.

فقد مثلت شبكة الإنترنت إحدى أدوات الجريمة العابرة للحدود وأحدثها، الأمر الذي يتطلب تعاوناً دولياً في مكافحتها. وقد جاء الإنترنت بكثير من الأنشطة غير المشروعة وسهل ارتكاب كثير من الجرائم، والإنترنت بوصفها نتاج المعلوماتية كأداة للربط والاتصال بين مختلف شعوب العالم تشكل أداة لارتكاب الجريمة أو محلاً لها وذلك بإساءة استخدامها على نحو غير مشروع الأمر الذي ينتج عنه ظهور طائفـــة جديدة من الجرائم عرفت بالجرائم المعلوماتية(تمام، 2000، ص270).

وتجدر الإشارة إلى أن هذه الأدوات تتعدد في الفضاء الإلكتروني وأهمها المواقـــع الإلكترونيـــة والبريد الإلكتروني (الفرع الاول)، والقرصنة والفيروسات الإلكترونية (الفرع الثاني).

الفرع الأول: المواقع الإكترونية والبريد الإلكتروني

أولاً: المواقع الإكترونية

يعرف الموقع الإلكتروني أنه معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل (Hyper text mark up language (HTML))، ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (WWW Browser)، ويقوم بحل رموز (HTML)، وإصدار التعليمات لإظهار الصفحات المتكونة. وتعد المواقع الإلكترونية من أهم الوسائل التي يمكن ممارسة الإرهاب الإلكتروني من خلالها، حيث يقوم الإرهابيون بإنشاء وتصميم بعض المواقع الخاصة بهم على الشبكة، وثم يستخدمون هذه المواقع في كثير من المجالات منها(السند، 2005، ص14-15):

- نشر أفكار الجماعة والدعوة إلى مبادئها
- تعليم طرق ووووسائل تنفيذ العمليات الإرهابية أو التي تساعد في تنفيذها، سواء العمليات الإرهابية التقليدية كتعليم صناعة المتفجرات، أو العمليات الإرهابية الإلكترونية كطرق اختراق البريد الإلكتروني للاخرين، وكيفية الدخول إلى المواقع المحجوبة، وطرق نشر الفيروسات، وكيفية اختراق وتدمير المواقع (كولن، 1999، ص26).
- تواصل المواقع مع بعضها البعض، اذ ترتكز الشبكة العنكبوتية أو ما يعرف بنظام الويب والمواقع على فكرة تخزين معلومات، والقدرة على إقامة صلات وعلاقات ترابطية مباشرة بين المواقع ببعض.
- توفر المواقع الإلكترونية أماكن التقاء أعضاء الجماعة، حيث يصعب التقاءهم في الواقع واختيار أماكن للالتقاء والتخطيط والتعليم والتدريب. حيث يسهل الإنترنت ذلك، ويمكن من التقاء أعضاء الجماعة والمتعاونين معهم من أماكن متعددة في وقت واحد لتبادل الآراء والخبرات والمعلومات وتلقي التدريبات اللازمة
- تمكن المواقع الإلكترونية من استقطاب المؤيدين للجماعة وأفكارها من خلال نشر أفكار الجماعة ومبادئها

ويمكن تحقيق هذه الأهداف من خلال مواقع الإنترنت وتطبيقاته المختلفة كالمنتديات وغرف الدردشة. وفي الواقع نجد أن الجماعات الإرهابية قد استفادت من مزايا الإنترنت والمواقع الإلكترونية

حيث نجد كثير من المواقع الخاصة ببعض التنظيمات والجماعات الإرهابية منتشرة على الشبكة وربما تعد هذه المواقع من أهم الانشطة و الوسائل المستخدمة في الإرهاب بشكل عام والإرهاب الإلكتروني بشكل خاص.

والمواقع المشبوهة عبارة عن مواقع كثيرة غير مرغوب فيها تنتشر على شبكة الإنترنت، منها ما يكون موجها ضد سياسة دولة أو ضد عقيدة أو مذهب معين، بحيث تهدف إلى تشويه صورة الدولة أو المعتقد المستهدف، من خلال تلفيق الأخبار والمعلومات من خلال إنشاء قاعدة بيانات بعناوين أشخاص يحصلون عليها من الشركات التى تبيع قواعد البيانات أو بطرق أخرى، ثم يقومون بإغراق تلك العناوين بمنشوراتهم ورسائلهم، لايصال أصواتهم إلى أكبر قدر ممكن، وهناك مواقع معادية للعقيدة منها ما يكون موجهاً من قبل أعداء حاقدين من أتباع الديانات الأخرى كمواقع الجاليات اليهودية أو النصرانية تحت مسميات إسلامية بقصد بث معلومات خاطئة عن الإسلام والقرآن، أو للدعاية للأديان الأخرى ونشر الشبهة والافتراءات حول الاسلام[8]. ومنها مواقع معادية للعقيدة داخل العقيدة الواحدة لكن لاختلاف المذاهب.

وقد كشف بعض خبراء الإرهاب الدولي كالأمريكي (جابريل ويمان)، عن زيادة كبيرة في عدد المواقع الإلكترونية التي تديرها المنظمات الإرهابية على شبكة الإنترنت العالمية، حيث قفز عدد تلك المواقع من 12 موقع عام 1998 إلى 4800 موقع في الآونة الأخيرة. ويشير الخبراء إلى أن الإرهاب الدولي أصبح أكثر خطراً وضراوة لاعتماده على التكنولوجيا الإلكترونية التي ساهمت في اتساع رقعة عملياتهم الإرهابية ومسرحها، وتطلب هذا الاتساع من الحكومات تخصيص موازنات كبيرة تقدر بملايين الدولارات لتعقب وتحليل المواقع الإلكترونية التابعة للجماعات الإرهابية. كما أن هذا النوع من الإرهاب باعتماده على التكنولوجيا قد ساعد المنظمات الإرهابية في التحكم باتصالاتهم وعزز حمايتهم وعدم اكتشافهم لسهولة قدرتهم على الاختباء والاختفاء. ونشر الكثير من المعلومات من خلال كتب ألفتها

---

8 من أمثلة هذه المواقع:

موقع: /http://www.answering-islam.org. وموقع: /http://www.aboutislam.com. وموقع: /http://www.thequran.com/.

جماعات إرهابية، ولم يكن بالامكان الحصول عليها، إلا أنه بالامكان الآن تحميلها من النت كاملةً، حيث صار لها دوراً كبيراً في الدعم الفكري للعمليات الإرهابية، وأصبح بامكان أي شخص في العالم الحصول عليها بدون ثمن (الصيفي، 2008، بدون رقم صفحة).

ومن أنماط المواقع الإلكترونية التي قد تمارس الإرهاب أو تعد وسيلة له أيضاً تلك المواقع المتخصصة بالقذف وتشويه سمعة الأشخاص، وهي مواقع موجهة ضد أشخاص محددين، تركز هجومها غالباً على ابراز سلبيات شخص مستهدف، بحيث تنشر بعض أسراره سواء التى يتم الحصول عليها بطريقة مشروعة أم غير مشروعة من خلال الدخول على جهازه والعبث به أو بتلفيق الاخبار عنه.

ومنها أيضاً المواقع الإباحية، حيث انتشرت الصور والأفلام الاباحية على شبكة الإنترنت بشكل كبير، مما شكل اهتماماً عالمياً بسبب الازدياد الهائل في أعداد مستخدمي الإنترنت حول العالم، فهناك مواقع وقوائم بريدية مخصصة لنشر الصور الجنسية بكافة أنواعها وأشكالها، والمواقع الاباحية غالباً ما يكون هدفها تحقيق الربح المادي، أما القوائم البريدية فهي غالباً مجانية يقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية، وهي أبعد عن المتابعة الأمنية. إذ أنها عبارة عن وسائل لتبادل الآراء والنقاش حول موضوع معين بين مجموعة من الأشخاص، وهي أشبه بنظام التخاطب عبر الإنترنت (ابراهيم، 2009، ص41).

وقد استفاد مرتكبي هذه الجرائم من شبكة الإنترنت حتى أصبح كل مستخدم للإنترنت معرض للتأثر بما يتم عرضه على الإنترنت الذي لا يعترف بأي حيز زماني أو مكاني وهذا ما يشكل خطراً على الصغار والكبار خاصة الاطفال.

وللحديث عن خصائص المواقع الفكرية المتطرفة التي تعد وسيلة من وسائل الإرهاب، وبشكل عام يمكن القول أن هذه المواقع تتسم بالآتي (نظمي، 2010، ص20):

- الشكل الفني في التصميم والحرفية وتقسيم الموضوعات.
- توفر الخدمات وتسهيل الوصول إلى المعلومات والتحديث المستمر للمحتوى ومواكبة الأحداث والتعليق عليها.

- استقطاب كتاب وفتاوى لعلماء معتبرون لرفع مستوى الثقة في المواقع.
- التنسيق العالي من هذه المواقع لنشر البيانات والخطب والمواد الجديدة التـي يقـدمها أحـد قـادة التنظيمات.
- صناعة نجوم هذه المنتديات ومؤازرتهم.
- توفير مواد سمعية ومرئية.
- تشجيع كتاب مذكرات من قبل المشاركين في بعض المناطق التي تنتشر بها العمليـات الإرهابيـة، لإلهام الشباب وتحفيزهم.
- تقديم خدمات إخفاء الأثر.
- تقديم شرح مفصل لاستخدامات البرامج والملفات والمواقع.
- تولية إدارة المواقع لأشخاص ذوي مقدرة متميزة وينتمون إلى بلدان مختلفة.
- تقديم عدة خيارات للزائر

ثانياً: البريد الإلكتروني

أما البريد الإلكتروني، فيعد أحد الخدمات التي تقدم من خلال شبكة الإنترنت، حيث يسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، ويعد من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما يمثله من سرعة في إيصال الرسالة من شخص إلى آخر، وسهولة الإطلاع عليها من قبل مستلمها، وفي أي مكان، لأن الرسالة لا ترتبط بمكان معين، بل يمكن الاطلاع عليها وقراءتها في أي مكان من العالم، ومن أي جهاز حاسب يرتبط بشبكة الإنترنت، ومن مظاهر التطور الآن إمكانية قراءتها من قبل الهاتف المحمول لتوافر خدمة اتصال الهاتف المحمول بالإنترنت، وقد أصبح البريد الإلكتروني من أكثر الوسائل والتطبيقات الإلكترونية استخداماً في مختلف القطاعات كونه الأكثر سهولة وأمناً وسرعةً في إيصال الرسائل، وهذا ما جعله الوسيلة الأكثر استخداماً في الإرهاب الإلكتروني، حيث يتم استخدامه للتواصل بين الإرهابيين وتبادل المعلومات بينهم. ويستخدم الإرهابيون البريد الإلكتروني في تبادل

الرسائل التي تتضمن نشراً لافكارهم والترويج لها بين جماعاتهم وأتباعهم. كما يستخدم البريد الإلكتروني للاختراق فقد يتمكن الإرهابيون من اختراق البريد الإلكتروني العائد لآخرين بالتالي الاطلاع على أسرارهم ومعلوماتهم وبياناتهم ومراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية (السند، 2005، ص10-11).

الفرع الثاني: الفيروسات والدودة والقنابل الإلكترونية والقرصنة

أولاً: الفيروسات

الفيروسات عبارة عن برامج حاسب آلية، إلا أن الأوامر المكتوبة فيها تكون أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما أو فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس، إصابة الجهاز به وقيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة فيه (الجنبيهي منير والجنبيهي ممدوح، 2005، ص68).

وهي برامج خبيثة تتسلل إلى البرمجيات تدخل إليها وتنسخ نفسها على برامج أخرى في الحاسب وتستخدم لغرضين هما(لطفي، 1993، ص496. ورستم، 1994، ص163):

1- غرض حمائي: لحماية البيانات والبرامج من خطر النسخ غير المشروع فينشط الفيروس لمجرد النسخ ويدمر نظام الحاسب الآلي الذي يعمل عليه.

2- غرض تخريبي: للدعاية والابتزاز والتخريب أو الحصول على منافع شخصية. وتكون هذه الفيروسات الخبيثة مرافقة ومخزنة على البرامج التطبيقية وبرامج التشغيل وتنشط في حالة نسخ البرامج ونقل المعلومات من الشبكة وتكون مختبأة داخل رسائل البريد الإلكتروني والوثائق والمعلومات التجارية والمالية عبر الشبكة، وتنتقل في حالة نسخ البرامج الحاصلة لها أو تحميل البيانات والمعلومات فتقوم بنسخ نفسها والسيطرة على نظام التشغيل حتى تتمكن من تعطيل

الجهاز بشكل كلي وقد تنسخ نفسها مراراً وتكراراً بحيث لا يمكن تشغيل البرنامج(الــشوابكة، 2004، ص238. والرومي، 2003، ص26).

بالتالي فهي برامج تعدل في البرامج الأخرى لتصبح نسخة منها، وهذا يعنى أن الفيروس ينسخ نفسه من حاسب آلي إلى آخر بحيث يتكاثر بأعداد كبيرة، ومن الجرائم المتعلقة بإرسال فيروسات حاسوبية قيام شخص أمريكي يدعى (Robert Morris) بإرسال فيروس في الثاني من نوفمبر عام 1988 عبر شبكة الإنترنت، حيث كرر الفيروس نفسه عبر الشبكة وأدى إلى تعطيل ما يقارب من 6200 جهاز حاسب آلي مرتبط بالشبكة، وقدرت الأضرار الناتجة عن ذلك بمئات الملايين من الدولارات(منشاوي، 1423هـ، ص11).

والفيروسات خمسة أنواع (الجنبيهي منير والجنبيهي ممدوح، 2005، ص71-72. وداود، 2000، ص134):

1. فيروسات الجزء التشغيلي للاسطوانة كفيروس (Brain) وفيروس (Newzeland)
2. الفيروسات المتطفلة: كفيروس (Cascade) وفيروس (Vienna)
3. الفيروسات متعددة الأنواع كفيروس (Spanish-Telecom) وفيروس (Flip)
4. الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز
5. حصان طرواده، وهو نوع مستقل بذاته ، ويشبه حصان طروادة لأنه يختفي تحت غطاء سلمي، إلا أنه ذو أثر تدميري خطير، حيث يعمل على اخفاء نفسه عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيير شكله، ويمكن مكافحته من خلال تحديث البرامج الخاصة بمكافحة الفيروسات بصفة دائمة. أما خــطــورة برامج حــصان طــروادة فتتمثل في (الجنبيهي منير والجنبيهي ممدوح، 2005، ص56):

أ. يعد من أخطر البـرامـج المـستـخـدمة من قبل المتسللين، لأنه يتيح الحصول على كلمات المرور (passwords)، وبالتالي السيطرة على الحاسب الآلي بالكامل.

ب. من خطورته أيضاً أنه لن يتم معرفته أو ملاحظة المتسلل كونه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز.

ج. أن معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات.

من الخطورة أيضاً أنه ذا طبيعة ساكنه تجعله أخطر من الفيروسات فهي لا تقوم بتقديم نفسها للضحية مثلما يـقـوم الفيروس بالتالي فإنه يقوم بمهمته التجسسية دون أي معارضة، الأمر الذي يجعل فرص إكتشافه ضئيلة.

كما تقسم الفيروسات حسب (الجنبيهي منير والجنبيهي ممدوح، 2005، ص72):

1. المكان المستهدف بالاصابة داخل جهاز الحاسب الآلي وهي ثلاثة أنواع تبعاً لذلك(الجنبيهي منير والجنبيهي ممدوح، 2005، ص72): فيروسات قطاع الاقلاع (Boot Sector) ، وفيروسـات المـلفات (File Injectors) ، وفيروسـات الماكرو (Macro Virus).
2. ومنهم من يقسمها إلى: فيروسـات الاصابـة المـباشـرة (Direct action) وهي الفيروسـات التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها. والفيروسات المقيمة (staying) وهي التي تظـل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمـر مـا، وتنـدرج معظـم الفيروسات المعروفة تحت هذا المسمى. والفيروسات المتغيرة (Polymorphs) وهي التي تقـوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلل برامج مكافحة الفيروسات.
3. ومن حيث العدوى تقسم أيضاً إلى أنواع: فيروس عام العدوى ينتقل إلى أي برنامج أو أي ملف ويهدف إلى تعطيل نظام التشغيل بشكل كامل. وفيروس محدد العدوى يستهدف نوعاً معيناً من النظم لمهاجمتها وهو بطيء الانتشار وصعب الاكتشاف. وفيروس عام الهدف يتميز بسهولة الإعداد واتساع مدى تدميره وغالبية الفيروسات من هذا النوع. وفيروس محدد الهدف: يعمل على تغيير الهدف من البرامج دون أن يعطلها ويحتاج إلى مهارة عالية ومنها ما يحدث تلاعباً مالياً أو

تعديل معين في التطبيقات العسكرية كحصان طروادة(محمد الجبور، 1993، ص276. وسلامه، 2006، ص162-165).

ثانياً: برامج الدودة

أطلق هذا البرنامج على الشبكة في الولايات المتحدة عام 1988، وسبب لأجهزة الحاسب على الشبكة الانهيار في قيادة وتوجيه الجامعات والمعدات العسكرية ومنشآت الأبحاث الطبية، ويقوم هذا البرنامج باستغلال أي ثغرة أو فجوة في نظم التشغيل كي ينتقل من حاسب إلى آخر ومن شبكة على أخرى عبر الوصلات التي تربط بينهما، وتتكاثر أثناء عملية الانتقال من خلال إنتاج نسخ منها وتهدف هذه البرامج إلى العمل على تقليل كفاءة الشبكة أو إلى التخريب العقلي للملفات والبرامج ونظم التشغيل لإشغال أي حيز ممكن من سعة الشبكة(ميلاد، 2007، ص99. والشوابكة، محمد أمين، 2004، ص193).

ثالثاً: القنابل المعلوماتية

تقوم هذه القنابل بأعمال تخريبية تحدد أوقاتها مسبقاً كإعداد برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين وبياناتهم اللازمة لدفع رواتبهم قبل استلام هذه الرواتب بوقت معين مما يؤدي إلى تأخير عملية الدفع وإرباك أعمال الشركة مثلاً وإساءة سمعتها. ومنها القنابل المنطقية التي تحدث أضراراً بالحاسب متى تم إجراء معين والقنابل الزمنية التي ترتبط بموعد محدد سلفاً تحدث الأضرار به (عوض، 1993، ص427. والشوا، 1994، 194).

رابعاً: القرصنة

تعد القرصنة من الممارسات والسلوكيات السيئة على الشبكة، وقد تشكل بذاتها جريمة جنائية يعاقب عليها القانون، وفي هذا المقام نتناولها كأداة جرمية لتنفيذ الجريمة الإرهابية الإلكترونية. والقرصنة هي الاستخدام أو النسخ غير المشروع لنظم التشغيل أو برامج الحاسب الآلي المختلفة، وبتطور وسائل التقنية تطورت وسائل القرصنة وأصبح من الشائع والسهل اليسير العثور على مواقع على شبكة الإنترنت خاصة بترويج البرامج المقرصنة مجاناً أو بمقابل مادي رمزي، وتسببت القرصنة بالحاق خسائر مادية فادحة وصلت عام 1988 إلى 11 مليار دولار امريكي في مجال البرمجيات وحدها (فادي، 1999، ص28-35. والجنبيهي منير والجنبيهي ممدوح، 2005، ص103-104).

المطلب الثالث: النتيجة الجرمية وعلاقة السببية في جريمة الإرهاب الإلكتروني

الفرع الاول: النتيجة الجرمية

إن النتيجة الإجرامية هي الأثر المترتب على السلوك الإجرامي، ويقدم الفقه الجنائي مدلولين للنتيجة الإجرامية هما(المجالي، 2010، ص215-217):

أ. المدلول المادي للنتيجة : وهو يُعبّر عن التغيير والتعديل الذي يطرأ في العالم الخارجي كأثر في السلوك الإجرامي ، ومثال ذلم أن الوفاة هي النتيجة المادية في جريمة القتل ، وإنتقال الحيازة هي النتيجة المادية في جريمة السرقة. وتجدر الإشارة هنا إلى أن النتيجة في مدلولها المادي ليست عنصرا لازما في جميع الجرائم ، مما درج الفقه على تقسيم الجرائم إلى : الجرائم المادية التي يتطلب المشرع فيها تحقيق نتيجة مادية ملموسه وبالتالي لا تكون الجريمة تامة إلا بوقوع النتيجة المنصوص عليها قانونا كالسرقة والقتل ، والجرائم الشكلية أو جرائم السلوك المجرد، وتعتبر تامة بمجرد إرتكاب السلوك الإجرامي دون إستلزام النتيجة مثل جرائم حمل السلاح بدون ترخيص أو جريمة إحراز المخدرات.

ب. المدلول القانوني للنتيجة : النتيجة في مدلولها القانوني هي الإعتداء على المصلحة التي يحميها القانون، سواء أدى الإعتداء إلى الإضرار بالمصلحة المعتدى عليها أو تهديدها بالخطر، فالنتيجة القانونية في جريمة القتل هي الإعتداء على حق الإنسان في الحياة وفي جريمة السرقة هي الإعتداء على حق الملكية . ويجري الفقه على تقسيم الجرائم وفق مدلولها القانوي إلى جرائم ضرر وجرائم خطر.

وبالنسبة للمصلحة المحمية في جرائم الإرهاب هي المصالح العليا في الدولة، لذا نجد أن بعض التشريعات تدرج الإرهاب ضمن الجرائم الماسة بأمن الدولة الداخلي كقانون العقوبات الأردني، وبعضها يدخلها ضمن الجرائم الماسة بشخصية الدولة كالتشريع الايطالي (خالد العازمي، 2007، ص81).

ويمكن الاستدلال على المصالح المحمية من القانون الأردني عندما عرف الإرهاب في المادة 147 بقولها:" استخدام العنف بأي وسيلة كانت أو التهديد باستخدامه، أياً كانت بواعثه وأغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي يهدف إلى تعريض سلامة المجتمع وأمنه للخطر إذا كان من

شأن ذلك إلقاء الرعب بين الناس وترويعهم أو تعريض حياتهم للخطر أو الحاق الضرر بالبيئة أو المرافق والأملاك العامة أو الأملاك الخاصة أو المرافق الدولية أو البعثات الدبلوماسية أو باحتلال أي منها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر أو إرغام أي حكومة أو أي منظمة دولية أو إقليمية على القيام بأي عمل أو الامتناع عنه".

ومن التعريف يمكن القول أن المصلحة المحمية في جريمة الإرهاب هي (النوايسة، عبدالاله2005، ص258. خالد العازمي، 2007، ص85-86):

أولاً: تجريم كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ إليه الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي. وهذا التجريم يتضمن حماية للنظام العام. وعدم تعريض سلامة المجتمع وأمنه للخطر.

ثانياً: كل استخدام للقوة أو العنف أو التهديد أو الترويع بقصد إشاعة الخوف والرعب بين عدد غير محدد من الناس"التخويف والرعب".

وبالنسبة للنتيجة الجرمية في جريمة الارهاب الالكتروني، فقد تناولت الباحثة فيما تقدم أدة الجريمة في الإرهاب الإلكتروني، وكيفية ممارسة وتنفيذ هذه الجريمة وركنها المادي أو النشاط المكون لها. أما بالنسبة للنتيجة الجرمية فيها فإنها ترتبط بشكل كبير بعنصر الخطر وتتعلق بالترويع والتخويف، ويستخدم لتحقيق هذه النتيجة وسائل نفسية تختلف عن كيفية ممارسة النشاط، إنما تكون مصاحبة له. ويطبق على هذه الوسائل وسائل السلوك الإجرامي الإرهابي. وهي تلك الوسائل التي تصاحب السلوك الإجرامي ويستخدمها الجاني وهي (العفيف، 2011، ص140-144. والعازمي، 2007، ص99-100):

1. القوة: وتشمل كل أنواع القهر أو الارغام أو الإكراه المادي متى كان من شأنها إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو أمنهم للخطر أو بالأملاك العامة أو الخاصة أو دور العبادة أو معاهد العلم أو تعطيل تطبيق الدستور أو القانون.

2. التهديد: أي زرع الخوف في النفس من خلال الضغط على إرادة انسان وتخويفه بأن ضررً سيصيبه أو يصيب أشخاصاً أو أشياءً ذات صلة به، ومن المعتقد أن له مصلحة في تفادي ذلك (حسني، 1988، ص981).

ولا يشكل التهديد بحد ذاته إرهاباً لأنه لا يعد كذلك إن لم يخرج إلى العالم المادي لكن في الجرائم الإرهابية يجب توافر عنصر الترويع والتخويف والازعاج. ومن هنا يأتي الربط بين الإرهاب وكثير من الجرائم التي قد تعد قائمة بحد ذاتها كالتخريب والاتلاف والقتل والإرهاب عبر الإنترنت وإثارة الفتن العرقية والداخلية فهي جرائم تقع ضمن دائرة الإرهاب لأنها تعبر عن استفزاز طوائف معينة وخلق نزاعات بين الاعراق(Dorothy E Dening،2000 من: بن يونس، 2004، ص649).

3. الترويع: أي إثارة الخوف والفزع الشديد والإحساس بالرعب والخطر الدائمين. ويقصد به أعلى درجات الخوف لأنه يخلق جواً عاماً لدى افراد المجتمع أو غالبيتهم أنهم يعيشون في رعب وخطر دائمين(نايل، 1996، ص18-19).

4. العنف: أي الشدة والقسوة في ارتكاب الأفعال الإجرامية، وفي مجال الأعمال الإرهابية يعني أفعال التدمير والتخريب والحاق الضرر والخسائر التي توجه إلى أهداف أو ضحايا مختارة أو ظروف بيئية أو وسائل أو أدوات يكون من شأن آثارها تعديل أو تقييد أو تحوير سلوك الآخرين في موقف المساومة والتي لها أثر في النظام الاجتماعي.

أما بالنسبة للنتيجة والتي تتحقق بكاملها، أي تتجاوز مرحلة الشروع بارتكاب الجريمة، فتتركز بالخطر القائم في الإرهاب الإلكتروني وأثره النفسي في المجتمع من خلال تحقيق عناصر الترويع

والتخويف ونشر الذعر بين الناس. وتنبع هذه النتيجة وترتبط بالخطر القادم من الفضاء الإلكتروني والذي سبق للباحثة الإشارة إلى جانب منه عند الحديث عن تحديات التكنولوجيا الحديثة بشكل عام وخطرها.

وتظهر النتيجة الخطرة في جريمة الإرهاب الالكتروني من ارتباطها بالآثار السلبية التي صاحبت ظهور الانترنت، فقد تغيرت أنماط الحياة بظهور الحاسبات الآلية وبسبب الاعتماد الكبير على وسائل تقنية المعلومات الحديثة في المؤسسات والمرافق العامة ومختلف المجالات التعليمي أو الأمني أو غير ذلك، لما لها من فوائد، إلا أنه ومقابل هذه الفوائد هناك وجه آخر لهذه التكنولوجيا، يتمثل في الاستخدامات والممارسات السيئة والضارة لها، ومن هذه الممارسات الإرهاب الإلكتروني الذي يهدد العالم بخطره المتمثل بسهولة استخدامه بشكل يمكن مستخدمه من القيام بأعمال إرهابية من منزله، أو مكتبه، أو في مقهى، أو أي مكان. ومن أخطاره عدم كفاية المنظومات الأمنية لمكافحته، فبالرغم من أن أكثر الأنظمة التقنية تقدماً وتطوراً هو المنظومة الأمنية إلا أنها أقل استقراراً وموثوقية بسبب تسارع وتيرة الجرائم الإلكترونية وأدواتها، وكثرة الثغرات الأمنية التي لا يمكن الحد منها على المدى الطويل، الأمر الذي استدعى العمل على تطوير أنظمة الأمن المعلوماتي في الإنترنت ليواكب التطور الحاصل في الجريمة الإلكترونية.

ويعتمد الإرهاب الإلكتروني ابتداءً على القدرة على اختراق شبكات الإنترنت لتحقيــق أهــداف عدوانية ذات طابع سياسي في الأغلب بالرغم من الآثار المختلفة الأخرى. ويرتبط الإرهاب الإلكترونـــي ويتطور بالتطورات التي حدثت وتحدث باستمرار في مجال المعلوماتية وما تتميز به مـــن خـــصائص ومقومات. كما تتعرض المجتمعات المعلوماتية الحديثة للأعمال الإرهابية بمختلف صورها وتتأثر بماينتج عنها من خسائر ودمار قد يلحق بمنظومة المعلومات التي تتحكم بحياة مجتمعات المعلوماتية والتي تعتمد على الكمبيوتر والإنترنت. وقد دفع الفضاء الإلكتروني الإرهابيين إلى استخدامه وسيلة لتحقيق مطـــالبهم وجرائمهم الإرهابية وأهدافهم لما يحققه الفضاء الالكتروتي من مزايا أهمهـــا عـــدم تعـــرض أعـــضاء الجماعات الإرهابية للخطر وصعوبة القبض عليهم (بوادي، 2004، ص116-117).

وقد أظهر بعض المنتمين للجماعات والتنظيمات الإرهابية قدرات كبيرة فـــي مجـــال الإنترنـــت والفضاء الإلكتروني أثناء استجوابهم على ارتكاب بعض الجرائم، وبسبب أهمية هذا النوع من الإرهـــاب

عمدت كثير من الدول ومنها الولايات المتحدة الأمريكية إلى إنشاء أجهزة شرطة خاصة بملاحقة مرتكبي جرائم الإرهاب الإلكتروني تحت مختلف المسميات حيث تسمى في الولايات المتحدة بشرطة الإنترنت والتي تختص بمتابعة الأنشطة الإرهابية الإلكترونية، وتتبع آثار الإرهابيين على أمل الوصول إليهم إذ أنهم لا يكتفون باستغلال شبكة الإنترنت العالمية للتخريب، والتجسس، أو السرقة، وإنما يقومون أيضاً باستغلال الشبكة العالمية لبث رسائلهم كاملة إلى ملايين الناس، وفي الوقت الذي يشاؤون بثها فيه، ومن أي مكان في العالم، كما قد تنطوي رسائلهم هذه على أوامر موجهة لبعض الجماعات للقيام بأعمال إرهابية معينة إذ أنه غالبا ما تحدث أعمال إرهابية كبيرة بعد بث رسائل معينة عبر الإنترنت (الصيفي، 2008، بدون رقم صفحة).

لهذا السبب أصبح الإرهاب الإلكتروني يمثل خطراً داهماً فقد أصبح هاجساً يخيف العالم بأسره، لسهولة استخدام التكنولوجيا ولشدة أثرها وضررها، وسهولة ارتكابه حيث بإمكان مرتكبه القيام به من منزله أو مكتبه أو أثناء جلوسه في مقهى أو مطعم، إذ اصبح العالم عرضة لهجمات الإرهابيين عبر الإنترنت، حيث يمارسون أنشطتهم التخريبية من أي مكان في العالم، وذلك في وقت لا تستطيع فيه التكنولوجيا الحديثة من حماية الناس من العمليات الإرهابية الإلكترونية، وذلك بالرغم من سعي العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أنها جهود غير كافية لمواجهة خطر هذا النوع من الإرهاب (السند، 2005، ص8-9).

وبالرغم من سرعة تطور الأنظمة التقنية الحديثة بما فيها الأنظمة الأمنية إلا أنها أقل الأنظمة استقراراً وموثوقية نتيجة للتسارع في وتيرة ارتكاب الجرائم الإلكترونية والثغرات الأمنية التي تساهم في ارتكابها والتي لا يمكن أن يتم الحد منها على المدى الطويل. وهذا يشمل بالطبع الإرهاب الإلكتروني الذي يعد أخطر الجرائم المعلوماتية، والذي أصبح خطراً يهدد العالم بأسره.

ومما يزيد من مخاطر هذه الجريمة أن العالم بأسره أصبح عرضة للهجمات الإرهابية عبر الإنترنت، وأن مرتكبيها أصبحوا يرتكبونها من أي مكان في العالم، ولأن التقنية الحديثة التي تعد هدف الجريمة أو بيئتها أو وسيلتها لم تعد وحدها قادرة على حماية الناس من العمليات الإرهابية الإلكترونية وخطرها الذي ظهر في آثار هذه الجريمة، حيث أضرت بشكل جسيم بالأفراد والمنظمات والدول. وقد

دفع ذلك الافراد والمنظمات والدول إلى اتخاذ إجراءات وتدابير واحترازات لمواجهته إلا أنها لـم تكـن كافية، وهناك حاجة ماسة لمزيد من الجهود لمواجهته.

وتعد الخسائر الناجمة عن الجرائم التقليدية بسيطة نسبياً بالمقارنة مع الخسائر التى تسببتها جرائم نشر الفيروسات، حيث تضر هذه الطائفة من الجرائم بالأفراد والشركات خاصة الـشركات الكبيـرة، إذ يمكن أن ينتج عنها توقف بعض أعمال تلك الشركات نتيجة لإتلاف قواعد بياناتها، وهـذه الفيروسـات تتراوح بين فيروسات عديمة الضرر أو ذات ضرر بسيط ومنها ذات أثر يدمر محتويات كامل الجهـاز، واتلاف البيانات التي يحتويها، وفي بعض المنشآت التجارية والصناعية قد يصل الضرر إلى درجة تكبد خسائر مادية ومبالغ كبيرة، ومثال ذلك وصلت خسائر فيروس كود رد إلى مليـاري دولار امريكـي، وخسائر فيروس الحب الشهير (8.7) مليون دولار (Ajeebb.com،8/8/2001) .

وحول أضرار الجرائم الإلكترونية بما فيها الإرهاب الإلكتروني، فقد ذكر المستشار محمد الألفي أن الإرهاب الإلكتروني يمكن أن يتسبب بإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات وقطع شبكات الاتصال المختلفة وتعطيل أنظمة الدفاع الجوي وإخراج الصواريخ عن مـسارها أو اختـراق الأنظمـة المصرفية أو إرباك حركة الطيران المدني وشل محطات الطاقة الحرارية والنووية وغير ذلـك (شـبكة الإعلام العربي :http://www.moheet.com/show_files.aspx?fid=137476).

ومن الجوانب الاقتصادية ما يمكن من اختراق مواقع البورصة العالمية وتهديد الإقتصاد الدولي، ويمكن من اختراق مواقع المطارات الدولية والتلاعب ببرامج الإتصالات بشكل يهدد سـلامة ووصـول الطائرات. ففي الولايات المتحدة الأمريكية تمكن أحد القراصنة من السيطرة على نظام الكمبيـوتر فـي مطار أمريكي صغير، وأطفأ مصابيح إضاءة ممرات الهبوط، مما هدد بحصول كارثة(الغـافري، د.س، بدون رقم صفحة).

وقد لا تتم النتيجة في جرائم الإرهاب الإلكتروني فتبقى الجريمة في طور الشروع، كما يعاقـب على المراحل النفسية والتحضيرية التي لا يعاقب عليها عادة بالنسبة للجرائم العادية، فيعاقب في جـرائم الإرهاب والإرهاب الإلكتروني على المؤامرة للقيام بالأعمال الإرهابية.

فمن المادة 107 من قانون العقوبات الأردني نجد أن المشرع الأردني قد جرم المؤامرة على القيام بالأعمال الإرهابية، وعرفت المادة المؤامرة بقولها:" المؤامرة هي كل اتفاق تم بين شخصين أو أكثر على ارتكاب جريمة بوسائل معينة".

وتظهر علة التجريم من مسلك المشرع الأردني في هذا المجال رغبته في القضاء على الأخطار المحدقة في الأعمال الإرهابية في مهدها، بالتالي فان المشرع الأردني قد تناول بالتجريم المرحلة النفسية المتمثلة بالعزم والتصميم، والمرحلة التحضيرية دون اشتراط البدء بالتنفيذ، خلافا لمنهجه هذا في باقي الجرائم(العفيف، 2011، ص63).

بالتالي يمكن القول أن المشرع قد عاقب على الشروع والتآمر للقيام بالأعمال الإرهابية، حيث جرم المشرع الأردني فعل التآمر على ارتكاب الأعمال الإرهابية وحدد للمتآمرين عقوبة. ويلاحظ أن المشرع قد تشدد إزاء جرائم الإرهاب بشكل عام وذلك من خلال سحب النطاق التجريمي ليس فقط إلى الأعمال التحضيرية للفعل إنما إلى المرحلة التي تسبق الأعمال التحضيرية متى اتخذت سمة وصفة التآمر على القيام بأعمال إرهابية (الجبور، 1993، ص276).

الفرع الثاني: علاقة السببية

لعلاقة السببية أهمية بالغة في كافة الجرائم التي لا يكتمل ركنها المادي بغير نتيجة إجرامية معينة تتميز بكيان مادي مستقل عن نشاط الجاني، ويتحقق بوقوعها مسؤولية عن جريمة تامة كما هو الشأن في جرائم الإعتدارء على الحياة. فعلاقة السببية هي التي تسند النتيجة الجرمية إلى الفعل، فتقرر بذلك توافر شرط أساسي لمسؤولية مرتكب الفعل عن هذه النتيجة، وهي بذلك تساهم في تحديد نطاق المسؤولية الجزائية في حال إرتباط النتيجة بالفعل إرتباطا سببيا. وإذا انتفت علاقة السببية فإن مسؤولية مرتكب الفعل تقتصر على الشروع إذا كانت الجريمة مقصودة وإذا كانت غير مقصودة فلا مسؤولية عنها ، وعليه فإن علاقة السببية تعتبر عنصرا في الركن المادي وشرطا لقيام المسؤولية الجزائية(المجالي، 2010، ص226).

وبالرغم من أن المشرع الأردني ترك معيار علاقة السببية للقضاء معتبرا أنها من صلب عمله ويفصل في كل قضية على حدة بحسب ظروفها وأحوالها(المجالي، 2010، ص230)، إلا أن المشرع أورد حكما خاصا في صلب (م245) عقوبات أنه :" إذا كان الموت والإيذاء المرتكبان عن قصد نتيجة أسابا متقدمة جهلها الفاعل وكانت مستقلة عن فعله أو لإنضمام سبب منفصل عن فعله تماما عوقب كما يأتي :

1- بالأشغال الشاقة مدة لا تقل عن عشر سنوات إذا كان فعله يستلزم عقوبة الإعدام أو الأشغال المؤبدة .
2- بتخفيض أية عقوبة مؤقتة أخرى حتى نصفها إذا كان فعله يستلزم عقوبة غير عقوبة الإعدام أو الأشغال الشاقة المؤبدة " .

ومن إستقراء النص يتبين لنا أن إقرار الشارع الأردني لنظرية تعادل الأسباب، أي أن مساهمة عوامل أخرى مع نشاط الجاني في إحداث النتيجة لا ينفي علاقة السببية بينهما، سوار كانت العوامل المتدخلة سابقة أو معاصرة أو لاحقة للفعل ، شريطة جهل الجاني بها.

وهناك أحكام عديدة صدرة عن محكمة التمييز الأردنية تفصح بوضوح عن إقرار نظرية تعادل الأسباب في مجال جرائم القتل والإيذاء المقصودين . ومن التطبيقات القضائية حسب منطوق نظرية تعادل الأسباب ما قضي به في حالة " إذا كان الإعتداء الذي قام به المتهم قد ألحق بإصبع المشتكية عاهة دائمة فإن إدانته بجناية إحداث العاهة متفق مع أحكام القانون، أما كون تجبير الاصبع قد جرى بصورة خاطئة فإن ذلك لا يؤثر في مسؤولية المتهم الجنائية، وإنما يمكن إعتباره سببا قانونيا مخففا طبقا لنص (م345) عقوبات على أساس أن العاهة لم تنتج عن مجرد الإعتداء وإنما بإنضمام سبب آخر وهو التجبير الخاطئ "(تمييز جزاء رقم72/127 ، مجلة نقابة المحامين ، العدد3 ، لسنة20 ، ص1616).

أما في مجال جرائم القتل غير المقصود ، فيبدو أن المحكمة العليا تتجه نحو إقرار السببية الملائمة، فقد قضت ان المعيار في توافر رابطة السببية بين الفعل الخاطئ والنتيجة (الوفاة) تقوم على عدم تصور وقوع النتيجة بإستبعاد الحطأ المرتكب ، ولغايات المسؤولية الجزائية لا فرق بين أن تكون رابطة

السببية مباشرة أو غير مباشرة عندما تكون العواقب متوقعة عادة من قبل هذا الخطأ (الفعـــل)(تمييز جزاء رقم75/87 ، مجلة نقابة المحامين، العددرقم1 لسنة24، ص641).

ويحتل مفهوم علاقة السببية أهمية بالغة في كافة خاصة تلك الجرائم التي لا يكتمل ركنها المادي بغير نتيجة إجرامية تتميز بكيان مادي مستقل عن نشاط الجاني، وتقوم بتحققها مـــسؤولية الجـــاني عـــن الجريمة التامة، بالتالي فإن علاقة السببية هي التي تسند الفعل للجاني وتسند النتيجة للفعـــل، وإذا انتفـــت علاقة السببية فإن مسؤولية الفاعل تقتصر على الشروع إذا كانت الجريمة مقصودة، فـــإن كانـــت غيـــر مقصودة فلا مسؤولية عنها لأنه لا شروع في هذه الجرائم، وهذا ما جعلها عنصراً من عناصـــر الـــركن المادي وشرطاً لقيام المسؤولية الجزائية (المجالي، 2010، ص217).

وتعد أحكام علاقة السببية واحدة في كافة الجرائم، فلا يوجد ما يميز علاقة السببية فـــي جريمـــة دون أخرى، إلا أن التشريعات تتفاوت في المعيار الذي تسند إليه وجود علاقة سببية وفي هذا الإطار نجد هناك الكثير من النظريات التي تبناها الفقه للتسهيل على القضاء في اثبات وجود علاقـــة الـــسببية بـــين الجرائم والنتائج المترتبة عنها. وهنا نتطرق للوضع في الأردن حيث لم يتطرق المشرع الأردني لوضع معيار عام لنظرية السببية، إلا أن محكمة التمييز تبنت في كثير من أحكامها ما يعرف بنظريـــة تعـــادل الأسباب(تمييز جزاء رقم 172/127، مجلة نقابة المحامين، العدد الثالث لسنة 20 ص1616).

وبما أن المشرع والقضاء الأردنيين لم يفردا معاييراً خاصة تتعلق ببعض أنواع مـــن الجـــرائم، بالتالي يمكن القول أن أحكام علاقة السببية تعد أحكاماً عامةً مما يعني انطباق هذه الأحكام فيمـــا يتعلـــق بجريمة الإرهاب والإرهاب الإلكتروني.

المبحث الثاني: الركن المعنوي في جريمة الإرهاب الإلكتروني والعقاب عليها

تناولت الباحثة في المبحث السابق الركن المادي لجريمة الإرهاب الإلكتروني بجميع عناصره: النشاط الإجرامي، والنتيجة، والعلاقة السببية، إضافة إلى أداة الجريمة التي تميزها، وكيفية ارتكابها، وفي هذا المبحث تتناول الباحثة الركن الثاني للجريمة لإكمال الحديث والبحث فيها، وهذا الركن هو الركن المعنوي، للانتقال إلى باقي أحكام جريمة الإرهاب الإلكتروني والبحث في صورها وأشكالها.

كما تتناول الباحثة في هذا المبحث المسؤولية الجزائية في جريمة الإرهاب الإلكتروني، والحماية الجنائية للمعلومات، لذا فإن الباحثة تتناول هذا المبحث من خلال المطالب الآتية:

المطلب الأول: الركن المعنوي في جريمة الإرهاب الإلكتروني

المطلب الثاني: المسؤولية على الشبكة الإلكترونية

المطلب الثالث: الحماية الجنائية لتكنولوجيا المعلومات

المطلب الأول: الركن المعنوي في جرائم الإرهاب الإلكتروني

أشارت الباحثة آنفاً أن للجريمة كيانين أولهما مادي ويتمثل في الركن المادي لها، وكيان نفسي وهو الركن المعنوي الذي يمثل الاصول النفسية لماديات الجريمة والسيطرة عليها، وبقدر سيطرة الارادة الجرمية على ماديات الجريمة تتعدد صور الركن المعنوي، ولإتجاه الإرادة الجرمية صورتان هما القصد الجرني حيث تكون الجريمة مقصودة، والخطأ الذي تتكون منه جريمة غير مقصودة(المجالي، 2010، ص325).

وقد ورد تعريف القصد الجرمي في قانون العقوبات الأردني على أنه نية إرتكاب الجريمة على ما عرفها القانون(المادة 63 من قانون العقوبات الأردني). ثم وضح المشرع الأردني القصد في المادة 64 عندما أفادت بأن الجريمة تعد مقصودة وإن تجاوزت النتيجة الجرمية الناشئة عن الفعل قصد الفاعل إذا كان توقع حصولها فقبل بالمخاطرة.

ويتكون الركن المادي من عنصرين هما العلم والإرادة، وعنصر العلم يعني علم الجاني بتوافر عناصر الجريمة كما عرفها القانون، والإرادة هي إرادة ارتكاب تلك العناصر وإرادة النتيجة التي تتحصل عنها(المجالي 2010، ص327-328).

بالتالي يمكن القول أن تكون الجريمة مقصودة أي أن الركن المعنوي يتخذ صفة القصد الجنائي فتوصف الجريمة أنها قصدية، وقد لا يقصد الجاني ارتكاب الجريمة لكنها تتحقق بالخطأ وتسمى الجريمة غير المقصودة.

وإذا ما أردنا تطبيق ذلك على الركن المعنوي في جريمة الإرهاب نجد أنها يتمثل أولا بعلم الجاني بالوقائع، أي عناصر الجريمة المكونة لها، والعلم بها كما عرفها القانون، أي العلم بالنصوص القانونية التي تجرم تلك الأفعال.

أما بالنسبة لعنصر الإرادة فيعني ذلك إرادة الجاني في جريمة الإرهاب تلك العناصر التي تتكون منها الجريمة الإرهابية أياً كانت صورها، ومن جانب آخر إرادة النتائج التي تترتب على الجريمة الإرهابية، بصرف النظر عن هذه النتائج إن كانت مادية أو معنوية.

وبمفهوم آخر فإن الركن المعنوي لجريمة الإرهاب هو أن يعلم الجاني بعناصر فعله، وبطبيعة الوسيلة التي يستخدمها في تنفيذ تلك الأفعال، ودورها في إحداث الذعر العام والتخويف، وانصراف إرادته إلى إتيان ذلك الفعل، مع علمه بما يحدث وانصراف إرادته إلى ذلك.

وما ينطبق على الإرهاب بصورته التقليدية ينطبق على الإرهاب الإلكترونية كجريمة مستحدثه وضمن الأفعال التي يتكون منها ركنها المادي وعناصره.

ومن النقاط ذات الأهمية في مجال الركن المعنوي أنه وبالنسبة للإرهاب لا يمكن تصور وقوع الجريمة بخطأ، فهي لا تكون إلا مقصودة، وكل الجرائم المقصودة يجب أن يتوافر لدى الفاعل القصد الجرمي العام بعنصريه: العلم والإرادة. كما أن المشرع يشترط في جريمة الإرهاب قصداً جرمياً خاصاً إضافة للقصد العام (نجم، 2000، ص246).

إذ أن الجرائم عادة تتكون من ركنين مادي ومعنوي، وهناك بعض الجرائم يتطلب لها المشرع ركناً معنوياً خاصاً يتمثل بالباعث أو الغاية من ارتكاب الجريمة، علماً بأن الأصل ألا يعتد المشرع بالباعث في الركن المعنوي للجريمة، إلا أنه وفي بعض الجرائم فإن المشرع ذاته يهتم بهذا الباعث ويشترطه لتوافر الركن المعنوي في تلك الجرائم.

ومن هذه الجرائم التي تتطلب قصداً خاصاً جريمة الإرهاب، وما ينطبق على هذه الجريمة ينطبق على جريمة الإرهاب الإلكتروني بطبيعة الحال، بالتالي يمكن القول أن جريمة الارهاب الالكتروني تتطلب كما سنرى قصداً خاصاً يتمثل بالاخلال بالنظام العام، أو تعريض سلامة المجتمع، أو أمنه للخطر.

بالتالي يمكن القول أنه وبالنسبة لجريمة الإرهاب الإلكتروني يمكن القول أنها كسائر الجرائم من حيث مدى توافر الأركان العامة للجريمة، وهي الركن المادي والركن المعنوي. ويتكون الركن المعنوي

فيها كسائر الجرائم من عنصري العلم والارادة. العلم بأركان الجريمة وعناصر كل ركن فيهـا، والعلـم بالوقائع، وبأنها تعد أفعالاً تشكل السلوك أو النشاط الجرمي لجريمة الإرهاب الإلكتروني، والعلم بالقوانين وهو العلم المفترض لأنه لا يعتد بالجهل بالقانون.

أما عنصر الارادة فيتكون من ارادة الفعل أي ارادة اتيان النشاط أو الفعل الذي يـشكل الـركن المادي للجريمة، وارادة تحقيق النتيجة الجرمية، حيث يمكن القول أن ارادة الجاني قـد انـصرفت إلـى تحقيقها.

ويتطلب المشرع الأردني توافر القصد الخاص إلى جانب القصد العام في جريمة القيام بأعمـال إرهابية، ويتمثل القصد الخاص في: الاخلال بالنظام العـام، أو تعـريض سـلامة المجتمـع، أو أمنـه للخطر(العفيف، 2011، ص148).

ومن أحكام محكمة أمن الدولة في مجال القصد الخاص ومجال الإرهاب الإلكتروني عامة، أنـه جاء في إحدى قراراتها:"...أما فيما يتعلق بالقصد الخاص لهذه الجريمة وهو قصد الاخلال بالنظام العـام أو تعريض سلامة المجتمع وأمنه للخطر المستفاد من نص المادة 147 فهو ثابت للمحكمـة مـن خـلال ظروف وملابسات هذه الدعوى والبينات المقدمة فيها وخاصة إفادة المتهم لدى المدعي العام التي اعترف من خلالها أنه عقد العزم على محاربة الأنظمة العربية ومن ضمنها الدوائر الحكومية الأردنية وذلك من خلال ارسال الرسائل التعديدية الإلكترونية قاصدً بذلك الاخلال بها وإثارة الخوف والفزع لدى العـاملين فيها..."(حكم محكمة أمن الدولة رقم 2005/131، تاريخ 2005/5/11، منشورات مركز عدالة).

ومع ذلك تبقى النصوص القانونية، بالرغم من سرعة تطور تكنولوجيا المعلومات، قاصرة عن الوفاء بأحكام المسؤولية الجزائية على شبكة الانترنت بشكل كامل، أو في بعض المسائل الحرجة، وذلك بسبب تعدد القائمين على الشبكة وتعدد أدوارهم، بحيث يصبح من السهل اثبات علاقة بعضهم بارتكاب بعض الجرائم، أو العكس، أي اثبات عدم تورطهم فيها.

المطلب الثاني: المسؤولية على الشبكة الإلكترونية

للمسؤولية الجنائية أحكامها العامة التي تطبق على كل الجرائم بشكل عام وهناك أحكام خاصة تتعلق بنوعية بعض الجرائم وخصوصيها كجرائم الارهاب التقليدي والارهاب الالكتروني، لذا تقوم الباحثة بتناول الاحكام العامة للمسؤولية الجزائية، قبل التطرق للمسؤولية على شبكة الانترنت كونها تتعلق بالارهاب الالكتروني الذي يتم من خلال الفضاء الالكتروني او بواسطته.

فالمسؤولية الجزائية هي الإلتزام بتحمل النتائج القانونية المترتبة على توافر أركان الجريمة، وموضوع هذا الإلتزام هو الجزاء الجنائي بصورة العقوبة أو التدبير الإحترازي الذي ينزله القانون بالمسؤول عن الجريمة. ويفترض نطاق المسؤولية الجزائية إستظهار الأساس القانوني والمنطقي والإجتماعي التي تقوم عليه، ثم بيان الأشخاص الذين يسألون مسؤولية جزائة كاملة والذين يسألون مسؤولية جزائية ناقصة (موانع المسؤولية الجزائية) (حسني، 1989، ص378).

أما بالنسبة ل**أساس المسؤولية الجزائية نجد أن منهج الشارع الأردني في تحديد أساس المسؤولية الجزائية** هو حرية الإختيار فالمجرم يسأل لأنه إختار الطريق المخالف للقانون ، لكن فريق من الفقهاء أنكر حرية الإختيار بحجة أن الإنسان مقدرة عليه تصرفاته (مذهب الجبرية)، إلا أن الشارع الأردني رجح مذهب حرية الإختيار وفقا للمادة (74) من قانون العقوبات الأردني، التي لا تجيز الحكم على أحد بعقوبة إلا إذا كان مرتكبها قد أقدم على الفعل عن وعي وإرادة ، وإعتبرهما شروطا للمسؤولية الجزائية. واستخلص الشارع إمتناع المسؤولية إذا انتفت الحرية لقوة غالبة أو إكراه معنوي أو ضرورة (المادتان 88 و89) أردني ، أو انتفى الوعي لصغر السن (المادة 36) من قانون الأحداث لسنة 2002 ، أو انتفى الوعي والحرية كالجنون (المادة 92) عقوبات أردني ، أو فقدان الوعي والإختيار للتسمم الناجم عن الكحول والعقاقير المخدرة (المادة 93) أردني(المجالي، 2010، ص388).

ورغم إعتناق الشارع الأردني لحرية الإختيار إلا أنه أقر في أحوال معينة بآراء المذهب الجبري ، فإذا كان قرر عدم مساءلة المجنون فإنه أنزل التدابير الإحترازية بحقه (المادة 1/92) أردني .

أما عناصرها فهي كالآتي(قريني علي، 2000، ص147. وص161):

الوعي والإدراك :

الوعي (Concience) يعني به الشارع التمييز والمقدرة على فهم ماهية الفعل وطبيعته وتوقع الآثار الناتجة عنه وعلى التفريق بين المحرم والمباح ، وتمر عملية الإدراك من الوجهة النفسية بمراحل ثلاثة : المستوى الطبيعي والإدراك الحسي ، والإدراك العقلي.

الإرادة :

ويعبر عنها بالقدرة على السيطرة على الفعل وبالإختيار وهي تعني التصميم الواعي للشخص على تنفيذ فعل معين ن وتصدر الإرادة " كنشاط نفسي واعي متجه إلى تحقيق غرض معين عن طريق وسيلة معينة". ولعل هذا المدلول هو ما قصده المشرع الفرنسي في قانون العقوبات الجديد عندما اشترط نص (المادة 1/122) في فقرتها الأولى : إنعدام التمييز أو قدرة الشخص على التحكم في أفعاله لإمتناع المسؤولية الجزائية بسبب الإضطراب العقلي أو العصبي .

أما بالنسبة ل**لمسؤولون جزائيا فإن الأصل فيها أن** الإنسان هو المسؤول جزائيا، وهذه هي القاعدة المسلم بها في الفقة الجزائي أن المسؤولية الجزائية لا ترتبط إلا بالإنسان الآدمي ، ورغم أن الشارع لم ينص عليها صراحة إلا أنه يفترضها بما تتضمنه نصوص القانون من أوامر ونواهي تتجه إلى الناس ، لأن الإفعال التي تجرمها نصوص القانون يفترض في صدورها عن الإنسان والعقوبات المقررة لها لا يتصور نزولها بغير إنسان، كما أنه مستحيل أن تتوافر أركان الجريمة والمسؤولية بالنسبة لغير الإنسان، فالإنسان هو وحده يملك القدرة على الإستجابة لأهداف المجتمع من تطبيق الجزاء الجنائي وعدم العودة بالتالي إلى إرتكاب الجريمة. ومع ذلك اتجهت بعض التشريعات الحديثة إلى تقرير مبدأ مسؤولية الأشخاص الإعتبارية او الهيئات المعنوية جزائيا ، وذلك بسبب إتساع دائرة نشاط الأشخاص في العصر الحديث ودخولها في معظم مجالات الحياة(المجالي، 2010، ص391).

إلا أن هناك مسؤولية للهيئات المعنوية أو الأشخاص الإعتبارية هي "مجموعة من الأشخاص والأموال التي تتمتع بالشخصية القانونية". وقد تقررت مسؤولية هذه الأشخاص أو الهيئات المعنوية جزائيا في القانون الأردني بمقتضى (المادة2/74) بقولها " تعتبر الهيئات المعنوية بإستثناء الدوائر الحكومية والهيئات والمؤسسات العامة مسؤولة جزائيا عن الجرائم التي يرتكبها مديروها أو ممثلوها أو وكلاؤها بإسمها أو لحسابها "(المجالي، 2010، ص392).

كما أن هناك **موانع للمسؤولية الجزائية، فقد** نص الشارع الأردني على موانع المسؤولية الجزائية (والتي عُبّر عنها بموانع العقاب) في القسم الثاني من الباب الرابع من الكتاب الأول في المواد (85-93) وحدد فيه أحكام الغلط والجهل بالقانون والواقع والقوة القاهرة وحالة الضرورة والجنون أو الإحتلال العقلي ثم الغيبوبة الناشئة عن الكحول والعقاقير المخدرة ، ثم تناول صغر السن كمانع للمسؤولية في (المادة36) من قانون الأحداث لسنة 1968 معدلا بقانون رقم 22 لسنة 2002 والذي يبين فيه الحداثة أو القصر سواء كان صغر السن مانعا للمسؤولية أم كان مخففا للعقوبة.

وفي ضوء ذلك نجد أن الشارع الأردني حصر موانع المسؤولية في الإكراه المعنوي وحالة الضرورة والجنون والتسمم الناتج عن تناول الكحول والعقاقير المخدرة وصغر السن إذا لم يكن الجاني قد بلغ سن السابعة . وقيام المسؤولية مرتبط بإجتماع شرطيها (الوعي والإرادة) اللذين يتضمنان في الوقت نفسة علتها ، فإذا انتفيا أو انتفى أحدها فقد انتفت كذلك علة المسؤولية وكان ضمنا إمتناعها.

ويمكن تناول أحكام المسؤولية من خلال تعداد كل من يساهم في تقديم خدمة الإنترنت كالآتي:

أولاً: مسؤولية متعهد الوصول

وهو الشخص الذي يقدم الخدمة الفنية عبر الإنترنت، ويلعب دور الوسيط في تقديم هذه الخدمة، ولا يتحمل هذا الشخص مسؤولية جزائية، أما مسؤوليته فتنحصر في المسؤولية العقدية فقط (النوايسة، نانسي، 2011، ص172).

وترى الباحثة في هذا الصدد أن العقاب على جريمة الإرهاب الإلكتروني، ونظراً لحجم الخطر الناجم عنها، يقتضي البحث -خلافاً لباقي الجرائم- في فكرة التوسع في المسؤولية الجزائية، وليس ذلك من باب التضييق من الحريات، إنما لخطورة جرائم الإرهاب عامةً، وجريمة الإرهاب الإلكتروني خاصةً. بالتالي يجب التوسع في وضع الالتزامات القانونية، وبالتوافق مع مبدا المشروعية، لكل من لهم علاقة بتقديم خدمة الإنترنت والاتصال على الشبكة، وهذا ما يمكن أن يعمم على جميع المسأهمين في تقديم الخدمة، سواء كان متعهد الوصول أم غيره.

ثانياً: مورد المعلومة

لا يشترط أن يكون مورد المعلومة هو مؤلفها أو ناشرها، إنما هو من يقوم بتجميعها حول موضوع محدد، إلا أنه مسؤول عن صحتها، لذا فإنه مسؤول عن احترام قواعد قانون العقوبات وحرمة الاعتداء على حياة الافراد (الرومي، 2004، ص127).

وتذهب الباحثة مع ذلك إذ يبقى مورد المعلومة مسؤولاً عن احترام قانون العقوبات عندما يمارس عمله في تجميع المعلومات حول موضوع محدد.

ثالثاً: مصدر مواقع الإنترنت

وهو من يحدد شكل الصفحة ويربط الصفحات ببعض وتتحدد مسؤولية من جانب اداري فقط (الصغير، 2002، ص134). وترى الباحثة فعلاً عدم وجود مسؤولية قانونية على مصدر مواقع الانترنت لأنه لا يطلع على مضمونها ولا يمتلك الوصول اليه او التحكم به.

رابعاً: مراقب الشبكات

وهو معني بمراقبة الشبكات واكتشاف المشاكل والأعطال فقط ولا مسؤولية جزائية عليه فيما يتعلق بالمعلومات(النوايسة، نانسي، 2011، س173).

خامساً: مدير موقع شبكة الإنترنت

وهو المعني بتشغيل وصيانة ومراقبة المواقع وما تحتويه من معلومات أو خدمات تقدم للمستخدمين ولا مسؤولية جزائية بحقه (النوايسة، نانسي، 2011، ص174).

سادساً: متعهد الاستضافة

وهو الشركة التي تستضيف مواقع الإنترنت على خوادمها مقابل الأجرة، وتتحمل المسؤولية الجزائية إن كانت تعلم أو عليها أن تعلم بالجريمة، ولم تتخذ الإجراءات اللازمة لوقفها (الرومي، 2004، 128).

ويأتي ذلك بالتوافق مع أحكام المسؤولية الجزائية وأركان الجريمة، ومع الواجبات الملقاة عليه، ومع توجه الباحثة نحو التوسع في إطار المسؤولية الجزائية، إلا أن الباحثة تتجه مع فرض نطاق محدد وضيق

من المسؤولية بالنسبة للأشخاص الذين لا تتطلب وظيفتهم العلم بوقوع جرائم من خلال الشبكة، أو من كان يعلم وقام باتخاذ الإجراءات اللازمة لمتع وقوعها، وهذا ما يتفق مع مبدأ المشروعية.

سابعاً: مزود خدمة الإنترنت

الذي يربط بين الاتصالات من ارسال واستقبال. وفيها جدل وحسب التشريعات المختلفة. فمنهم من يقيم مسؤوليته ومنهم من لا يحمله المسؤولية الجزائية إنما على أساس المسؤولية الادارية فقط (يونس، 2004، ص758 وما بعدها).

وفي الأردن فإن مسؤولية مزود الخدمة الجزائية تظهر من نص المادة 75 ب من قانون الاتصالات الأردني التي تنص على أنه:" كل من قام أو ساهم بتقديم خدمات اتصالات مخالفة للنظام العام أو الآداب العامه يعاقب بالعقوبات المنصوص عليها بالفقرة (أ) من هذه المادة بالإضافة إلى تطبيق الأحكام المنصوص عليها في المادة (40) من هذا القانون ". ويشمل ذلك بالطبع مزود الخدمة. ويرى البعض شموله لمقاهي الإنترنت (النوايسة، نانسي، 2011، 96).

كما يحمل القضاء الأردني المواقع الإلكترونية المسؤولية استناداً لقانون المطبوعات والنشر رقم 5 لسنة 2010[9]، حيث تنص المادة 24/ج على أنه:" في حال غياب رئيس التحرير الأصيل أو من يقوم بعمله يعتبر مالك المطبوعة الصحفية أو مصدرها مسؤولاً مسؤولية كاملة عما ينشر فيها إلى أن يباشر رئيس التحرير الجديد عمله ". والمادة 41 على أنه:" يحظر على كل من المطبوعة المتخصصة ودار الدراسات والبحوث أو دار قياس الر أي العام أو كل من اعتاد العمل فيها تلقي أو قبول أي معونة أو مساعدة أو هبة مالية أو تمويل من جهة أردنية أو غير أردنية ولايشمل ذلك تمويل المشاريع المشتركة أو الدراسات أو الأبحاث التي يوافق عليها الوزير".

---

9 صدر قرار قضائي عن محكمة التمييز بتاريخ 2010/1/13 يقضي بإخضاع المواقع الإلكترونية إلى قانون المطبوعات والنشر، على اعتبار أن "الموقع الإلكتروني يعتبر من وسائل النشر التي تدون فيها الأفكار، والمعاني والكلمات وبأي طريقة كانت، ووفق القرار فإن الموقع الإلكتروني هو وسيلة من الوسائل التي يتم فيها تدوين هذه الأفكار والمقالات ونشرها، ما صنف المواقع الإلكترونية ضمن المطبوعات، وفقا لتعريف المطبوعة الوارد في المادة الثانية من قانون المطبوعات والنشر، مما يوجب على الحكومة البحث عن وسائل قانونية لضمان عدم تقييد حق ممارسة المواقع الالكترونية لحرية الرأي والتعبير: www.eyeonmediajo.net/?p=3321

حيث جاء في قرار محكمة التمييز الشهير أنه:"1. يستفاد من نص المادة الثانية من قانون المطبوعات والنشر أن هناك نوعين من المطبوعات أشار إليهما المشرع في هذه المادة وهما: النـــوع الأول: ويشمل المطبوعة بشكل عام وقد عرفها المشرع بأنها كل وسيلة نشر دونت فيها المعاني أو الكلمات أو الأفكار بأي طريقة من الطرق، والنــوع الثانــي: ويشمل المطبوعة الدورية وهي المطبوعة الصحفية المتخصصة بكل أنواعها والتي تصدر في فترات منتظمة.

وأن مناط الفصل في هذه الدعوى يتوقف على بيان ما إذا كان الموقع الإلكتروني يعتبر مطبوعة وفقاً لتعريف المطبوعة الوارد في قانون المطبوعات والنشر أم لا ؟. وفي هذا فانه إذا كان النوع الثاني لا يتسع نطاقه لشمول المواقع الإلكترونية على اعتبار أن هذا النوع وحسبما جاء بتعريف المشرع للمطبوعة الدورية بأنها تقتصر على المطبوعات الصحفية التي تصدر في فترات منتظمة ولا يعتبر الموقع الإلكتروني بأي حال من الأحوال مطبوعة صحفية ، فإن النوع الأول يتسع نطاقه لشمول المواقع الإلكترونية ، على اعتبار أن هذا النوع وحسبما جاء بتعريف المشرع للمطبوعة بأنها كل وسيلة نشر تدون فيها الأفكار والكلمات بأي طريقة كانت، وفي هذا فإن الموقع الإلكتروني هو وسيلة من الوسائل التي يتم فيها تدوين الأفكار والمقالات ونشرها، وبالتالي فإن المواقع الإلكترونية تعتبر من المطبوعات وفقاً لتعريف المطبوعة الوارد في قانون المطبوعات والنشر وتخضع لأحكامه. كما أن المادة الخامسة من ذات القانون وعندما نصت على ما يتوجب على المطبوعـــات القيام بـــه من احتـــرام الحقيقة والامتناع عن نشر ما يتعارض مع مبادئ الحرية ...نصت على المطبوعات بشكل عام وحسبما جاء بالتعريف العام للمطبوعة وليس كما جاء بتعريف المطبوعة الدورية الأمر الذي يستخلص منه أن المشرع ميز في هذا القانون بين نوعين من المطبوعات ، المطبوعات بصفة عامة والمطبوعات الدورية بصفة خاصة وأن المواقع الإلكترونية تدخل ضمن تعريف المطبوعات بصفة عامة وتخضع لأحكام قانون المطبوعات والنشر"(قرار تمييز جزاء رقم : 1729 /2009 تاريخ 2010/1/10).

المطلب الثالث: الحماية الجنائية لتكنولوجيا الاتصالات

لم يكن هناك قانون معين في الأردن ينظم جميع الأحكام الخاصة بالحماية الجنائية لتكنولوجيا الاتصالات، ويكون خاصاً للجرائم الإلكترونية. حيث كانت تتشتت نصوص هذه الحماية في كل من: قانون الاتصالات رقم 13 لسنة 1995، وقانون المعاملات الإلكترونية لعام 2001، وقانون الاعلام المرئي والمسموع رقم 71 لسنة 2002، وقانون توظيف موارد تكنولوجيا المعلومات رقم 81 لسنة 2003. إلا ان المشرع الأردني في العام 2010 أصدر قانون جرائم أنظمة المعلومات المؤقت لعام 2010.

وتدور فكرة الحماية الجزائية في هذه التشريعات حول بعض جرائم تكنولوجيا المعلومات، ولم يكن هناك أي ظهور لجريمة مستقلة تتعلق بالإرهاب الإلكتروني في القوانين السابقة لقانون جرائم أنظمة المعلومات المؤقت لعام 2010، إنما جاءت لتجريم أفعال وصور الاعتداء على تكنولوجيا المعلومات. وقد آثرت الباحثة استعراض هذه الجرائم والعقوبات المفروضة عليها. وكالآتي:

أولاً: الحماية الجنائية في مرحلة ما قبل قانون جرائم أنظمة المعلومات المؤقت لعام 2010

1. الحماية الجنائية في قانون الاتصالات:

وقد ورد فيه تجريم كثير من الأفعال ضمن الأوصاف الجرمية الآتية:

أ. جريمة نشر أو اشاعة مضمون الاتصالات دون مسوغ قانوني، حيث تنص ويعاقب عليها بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (100) دينار ولا تزيد على (300) دينار أو بكلتا العقوبتين(المادة 71).

ب. جريمة تخريب منشآت الاتصالات، ويعاقب عليها بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل على (200) دينار ولا تزيد على (5000) دينار أو بكلتا العقوبتين، وتضاعف العقوبة إذا تسبب فعله بتعطيل حركة الاتصالات(الفقرة أ من المادة 72).

ج. جريمة اتمام الاتصالات بوسائل غير مشروعة وجريمة تخريب أجهزة الاتصالات العامة، ويعاقب عليها بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (50) دينار ولا تزيد على (200) دينار أو بكلتا العقوبتين(المادة 73).

د. جريمة تقديم خدمات الاتصالات بشكل غير مشروع واستغلالها لاغراض غير مشروعة، ويعاقب عليها بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (300) دينار ولا تزيد على (2000) دينار أو بكلتا هاتين العقوبتين(المادة 75).

ه. جريمة اعاقة أو اعتراض وسائل شبكات الاتصالات، ويعاقب عليها بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على (200)دينار أو بكلتا العقوبتين(المادة 76).

و. جريمة اخفاء الرسائل أو رفض نقلها أو افشائها، يعاقب عليها بالحبس لمدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على (1000) دينار أو كلتا العقوبتين(المادة 77).

ز. جريمة إنشاء أو تشغيل أو ادارة شبكات الاتصالات العامة بالمخالفة للقانون ويعاقب عليها بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (5000) دينار ولا تزيد على (25000) دينار أو بكلتا هاتين العقوبتين(المادة 78/أ).

ح. جريمة استخدام الشبكات العامة أو الخاصة بطريقة غير قانونية ويعاقب عليها بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر أو بغرامة لا تقل عن (2000) دينار ولا تزيد على (5000) دينار أو بكلتا هاتين العقوبتين(المادة 79).

ط. جريمة اعتراض الموجات الراديوية أو التشويش عليها ويعاقب عليها بالحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن (5000) دينار ولا تزيد على (25000) دينار أو بكلتا هاتين العقوبتين ."

ي. جريمة استخدام الموجات الراديوية عمداً بدون ترخيص ويعاقب عليها بالحبس مدة لا تقل عن شهر أو بغرامة لا تقل عن (2000) دينار ولا تزيد على (5000) دينار أو بكلتا هاتين العقوبتين(المادة 2/80).

ك. جريمة إدخال أجهزة الاتصالات بالمخالفة للقانون ويعاقب عليها بالحبس لمدة لا تزيد على شهر أو بغرامة لا تقل عن (100) دينار ولا تزيد على (500) دينار (المادة 81).

ل. جريمة إدخال أجهزة مخالفة للقواعد الفنية وبها معلومات غير صحيحة ويعاقب عليها بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (100) دينار ولا تزيد على (2000) دينار أو بكلتا هاتين العقوبتين(المادة 82).

م. جريمة تشغيل محطات راديوية أو الاحتفاظ بها بالمخالفة لأحكام قانون الاتصالات ويعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر أو بغرامة لا تقل عن (100) دينار ولا تزيد على (500) دينار أو بكلتا العقوبتين (المادة 83).

تلاحظ الباحثة من هذه الجرائم الواردة في قانون الاتصالات أنها لم تتطرق لجريمة الإرهاب الإلكتروني، ولم تتطرق للأفعال التي قد تساهم في تحقيقها، إنما هي تجريم لبعض الجرائم المستحدثة التي ترتكب من خلال تكنولوجيا المعلومات والاتصالات. إلا أن ذلك لا ينفي أن هذه الجرائم والافعال قد تصاحب جريمة الارهاب الالكتروني أو انها قد تدخل في باب الركن المادي لها عندما يتم القيام بأعمال ارهابية من خلال وسائل تكنولوجية. فبالنظر الى تلك الافعال نجد ان الفاعل في جرائم الارهاب سواء التقليدي او الالكتروني قد يلجأ الى نشر أو اشاعة مضمون الاتصالات، وتخريب منشآت الاتصالات، واجراء اتصالات غير مشروعة وغير ذلك من جرائم.

إلا أن الاشكالية تكمن في مدى الذهاب باتجاه تجريم هذه الأفعال إن كان بشكل مستقل أم باعتبارها من الأفعال المكونة لجريمة الارهاب الالكتروني، فبالنظر الى العقوبات التي أقرها المشرع لهذه الافعال نجد انها تتضاءل أمام الخطورة الكامنة في جريمة الارهاب. خاصة في ظل عدم وضوح جريمة الارهاب

بشكل عام من حيث التعريف والتجريم وجريمة الارهاب الالكتروني ايضاً وفي ظل تشعب صور هذا النوع من الارهاب. حيث يجب على القائمين بالتحقيق الحذر في مدى ربط هذه الافعال بجريمة الارهاب الالكتروني.

2. الحماية الجنائية في قانون الاعلام المرئي والمسموع

وقد ورد في هذا القانون تجريم بعض من الأفعال ضمن الأوصاف الجرمية الآتية:

أ. جريمة ادخال المصنفات دون اذن هيئة الاعلام المرئي والمسموع الأردني[10].

ب. جريمة عرض أو تداول المصنفات دون موافقة هيئة الاعلام المرئي والمسموع ويعاقب عليها بمدة لا تقل عن أسبوع ولا تزيد على ستة أشهر أو بغرامة لا تقل عن خمسمائة دينار ولا تزيد على خمسة آلاف دينار أو بكلتا هاتين العقوبتين ومصادرة المصنف وإغلاق دار العرض حسب مقتضى الحال، وإذا تكررت المخالفة تضاعف العقوبة وتلغى بقرار من الهيئة رخصة التداول في حالة تكرار المخالفة أكثر من مرة (المادة 27 و28).

ج. جريمة ممارسة أعمال البث دون الحصول على ترخيص، ويعاقب عليها بمدة لا تقل عن سنة ولا تزيد على خمس سنوات أو بغرامة لا تقل عن خمسة وعشرين ألف دينار ولا تزيد على مائة ألف دينار أو بكلتا هاتين العقوبتين ومصادرة جميع المعدات والأجهزة المستخدمة وإزالة الضرر الناشيء عن المخالفة. وتضاعف العقوبة في حال تكرار المخالفة(المادة 29/أ).

10 تنص المادة 26 على أنه " أ- بإستثناء المصنفات التي يتم إدخالها لغرض الإستعمال الشخصي، لا يجوز إدخال أي مصنف إلى المملكة بهدف التداول إلا بعد الحصول على إجازة مسبقة للمصنف. ب- تحدد أسس إجازة المصنفات وشروط منح رخص تداولها ورقابة هذا التداول والإعفاء من الإجازة أو رخص التداول بموجب نظام يصدر لهذه الغاية كما تحدد بمقتضاه رسوم إجازة المصنفات ورخص تداولها ".

د. جريمة ممارسة أعمال البث أو اعادة البث بالمخالفة لشروط الترخيص ويعاقب عليها بغرامة لا تقل عن عشرة آلاف دينار ولا تزيد على خمسين ألف دينار مع إلزامه بالتعويض وإزالة الضرر الناشيء عن المخالفة، ويحق للهيئة إيقاف البث مدة لا تزيد على شهرين. وتضاعف العقوبة في حال إستمرار المخالفة أو تكرارها ولمجلس الوزراء بناء على تنسيب الوزير المستند إلى توصية المدير إلغاء رخصة البث الممنوحة للمرخص له وإلزامه بتعويض الهيئة بما لا يقل عن الرسوم السنوية المستحقة على رخصة البث الملغاة(المادة 29/ب).

ثانياً: الحماية الجنائية في قانون جرائم أنظمة المعلومات المؤقت لعام 2010

تطور الأمر فيما يتعلق بجريمة الإرهاب غي هذا القانون إذ يعد أول قانون يتطرق لجريمة الإرهاب او القيام باعمال تساعد في تنفيذ عمليات إرهابية، حيث تتناول الباحثة الصور التجريمية للجرائم التي جاء بها هذا القانون ومن ثم تقف عند النص الخاص بالإرهاب، كالآتي:

1. الجرائم العادية، حيث جاء فيه تجريم الأفعال الآتية:

أ. الدخول قصداً إلى موقع إلكتروني أو نظام معلوماتي بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، ويعاقب عليها بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين (المادة 3/أ). وإذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين (الفقرة ب من المادة الثالثة).

ب. الادخال أو النشر أو الاستخدام القصدي لبرنامج عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل

أو نسخ أو التقاط أو تمكين الاخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح، ويعاقب عليها بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين (المادة الرابعة).

ج. الالتقاط أو الاعتراض أو التصنت قصداً وبوجه غير مشروع على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين (المادة الخامسة).

د. الحصول قصداً دون سبب مشروع عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات بطاقات الائتمان أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية، ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار أو بكلتا هاتين العقوبتين (الفقرة أ من المادة السادسة).

ه. استخدام عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات بطاقات الائتمان أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الاخرين، ويعاقب عليها بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار (الفقرة ب من المادة السادسة)[11].

و. إرسال أو نشر بيانات أو معلومات قصداً عن طريق الشبكة المعلوماتية أو أي نظام معلومات تنطوي على ذم أو قدح أو تحقير أي شخص يعاقب بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (2000) ألفي دينار (المادة الثامنة).

---

11 تجدر الاشارة إلى انه لغاية هذه الجريمة على الترتيب اعلاه فنه تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) إلى (6) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأديته وظيفته أو عمله أو بسببها: المادة السابعة من ذات القانون.

ز. الإرسال أو النشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي مناف للحياء موجه إلى أو يمس شخصا لم يبلغ الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة ألاف دينار(المادة 9/أ).

ح. القيام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية تتعلق بتحريض من لم يبلغ الثامنة عشرة من العمر أو استغلاله في الدعارة والأعمال الإباحية أو التشهير به أو بيعه أو تحريضه على الانحراف أو تسخيره في ارتكاب جريمة، ويعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة الاف دينار(المادة 9/ب).

ط. القيام قصداً باستخدام الشبكة المعلوماتية أو أي نظام معلومات للترويج للدعارة أو الفجور يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار(المادة العاشرة).

2. الجرائم المتعلقة أو المرتبطة بالإرهاب، وقد أورد هذا القانون صورتين:

أ. الإرسال أو النشر قصداً عن طريق نظام المعلومات أو الشبكة المعلوماتية بيانات أو معلومات أو أنشئ موقعاً إلكترونياً *لتسهيل القيام بأعمال إرهابية أو الاتصال بجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو ترويج أفكارها، أو تمويلها، فيعاقب بالأشغال الشاقة المؤقتة* (المادة 11).

ويلاحظ أن الركن المادي لهذه الجريمة يتمثل في إرسال بيانات أو معلومات أو نشرها قصداً عن طريق نظم المعلومات أو الشبكة المعلوماتية لتسهيل القيام يأعمال إرهابية أو لتسهيل الاتصال بجماعة ارهابية أو بجمعية تقوم بأعمال ارهابية أو تسهيل ترويج أفكارها أو تمويلها.

كما يلاحظ ان المشرع قد تشدد في عقوبة هذه الجريمة إذ جعلها الأشغال الشاقة أي ما بين 3 سنوات و15 سنة على خلاف العقوبات التي وردت للأفعال الأخرى التي كان حدها الأعلى يصل الى السنتين.

ب. الدخول قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة ألاف دينار(المادة 12/أ). وإذا كان هذا الدخول بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو بث أفكار تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار(المادة 12/ب).

ويلاحظ على هذه الجريمة أنها تقترت الى حد كبير من الجرائم الارهابية خاصة في الشق الثاني منها وهو الدخول قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، وذلك بهدف إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو بث أفكار تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، حيث عاقب المشرع على هذه الجريمة بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

وبالنظر إلى النشاط الجرمي الذي تتكون منه هذه الجريمة نجد أنه يتشابه مع يعض الأنشطة الإرهابية في أكثر من جانب، فمن حيث أداة الجريمة ووسيلة ارتكاب النشاط الارهابي، ومن حيث اعتبار الفضاء الالكتروني بيئة للجريمة، ومن حيث تأثيرها ومساسها بمصالح المجتمع العليا وهي الأمن والسكينة خاصة الأمن الوطني لما فيه من تحقيق للمصلحة العامة.

تجدر الإشارة أخيراً إلى أنه ومن خلال النظر إلى تلك الجرائم نجد أنها، وكما اتضح في مختلف مواضع دراستنا، أن منها ما يتعلق بجرائم المعلومات بشكل عام، ومنها ما صب مباشرة –ولأول مرة– في باب الإرهاب الإلكتروني، وهنا تتمنى الباحثة على المشرع التوسع في ذلك وتأسيس باب مستقل لتأسيس نظرية العقاب على الجرائم الإرهابية الإلكترونية وأحكامها.

كما تجدر الإشارة إلى أن هذا القانون لم يغفل أحكام المساهمة الجرمية، وصلاحيات الضابطة العدلية وجهات التحقيق في هذه الجرائم ووضع الأحكام الخاصة لها، وأحكام الادعاء بالحق الشخصي من قبل المضرور من تلك الجرائم.

تجدر الإشارة إلى أن أكثر التشريعات وضوحاً وتميزاً في مجال تجريم الإرهاب عبر الإنترنت، هو التشريع الفرنسي: حيث تنص المادة 1/421 من قانون العقوبات الفرنسي على أنه:"تعد أعمالاً إرهابية حين تكون تلك الأعمال ذات علاقة بمشروع فردي أو جماعي يهدف إلى الاخلال بشكل خطير بالنظام العام بالترويع أو بالرعب، الأعمال الإجرامية الآتية: ...، السرقة، الابتزاز، التدمير، التجريد، الاتلاف، وكذلك الجرائم في مجال المعلوماتية حسب تعريفها في الكتاب الثالث من هذا القانون".

ويرتكب الإرهاب من قبل الأفراد الطبيعيين (المادة 3/422 من قانون العقوبات الفرنسي)، كما يقبل أن يكون الشخص المعنوي مرتكباً لجريمة إرهابية (المادة 2/121 من قانون العقوبات الفرنسي). بالتالي – وحسب القانون الفرنسي– تعد كل الأفعال التي قررتها المادة 1/323 من قانون العقوبات الفرنسي والتي تمثل عدواناً على نظم المعالجة الآلية للبيانات أعمالاً إرهابية متى حدثت وارتكبت بشكل يمثل اخلالاً كبيراً وخطيراً بالنظام العام سواء ارتكبها أفراداً طبيعيين أو أشخاص معنويين (بن يونس، 2004، ص651).

كما عالج المشرع الفرنسي ذلك في المادة ذاتها في القرة 3 (3/323) من قانون العقوبات، والتي تقضي بتجريم ادخال أي بيانات في نظم المعالجة الالية أو تدمير أو تعديل البيانات التي يحتويها أو طريقة

معالجتها. فيلاحظ بالتالي أن المشرع الفرنسي قد حدد صور السلوك الجرمي المكـــون للـــركن المـــادي للجريمة(ميلاد، 2007، ص42-43).

المبحث الثالث: صور وأشكال الجرائم الإرهابية في الفضاء الإلكتروني

أشارت الباحثة في أكثر من موضع من هذه الدراسة إلى أن الكمبيوتر يلعب ثلاثة أدوار في الحقل الجنائي: فقد يكون هدف الجريمة عند توجيه السلوك الجرمي للحصول على المعلومات بدون تصريح أو الحاق الضرر بالمعطيات أو بنظام الكمبيوتر أو شبكة الكمبيوتر، كتوجيه الفيروسات والديدان التقنية من قبل الهاكرز. وقد يكون وسيلة ارتكاب الجريمة، كالتزوير والاحتيال باستخدام الكمبيوتر. وقد يكون الكمبيوتر بيئة ارتكاب الجرم كتخزين معلومات عن أنشطة إجرامية والتحريض وإثارة الفتن(يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، **ص**29).

ونلاحظ بالنسبة للإرهاب الإلكتروني أنه قد يغطي الصور الثلاثة. ويعد من أهم مخاطر الإنترنت، ففي عصر الازدهار الإلكتروني وقيام الحكومات الإلكترونية، تبدلت أنماط الحياة بما في ذلك أنماط الجريمة، رغم أن الجرائم احتفظ أغلبها بمسمياتها التقليدية إلا أن التغيير صار في طرق ارتكابها، ومن هذه الجرائم جريمة الإرهاب التي اخذت اتجاهاً جديداً يتماشى مع التطور التقني.

وقد انتبه الغرب لجريمة الإرهاب الإلكتروني مبكراً، حيث شكل الرئيس الامريكي بيل كلنتون لجنة خاصة لحماية البنية التحتية الحساسة في أمريكا، حيث قامت هذه اللجنة بداية بتحديد الأهداف المحتمل استهدافها من قبل الإرهابين كمصادر الطاقة الكهربائية والاتصالات وشبكات الحاسب الآلي، وفي خطوة تالية تم إنشاء مراكز خاصة في كل ولاية للتعامل مع الأخطار المحتملة من هجمات إرهابية إلكترونية. ثم قامت وكالة الاستخبارات المركزية بإنشاء مركز خاص بالحروب المعلوماتية التي وظفت به كثير من خبراء أمن المعلومات، كما شكلت قوة ضاربة متخصصة لمواجهة الإرهاب الإلكتروني على مدار الساعة في وكالة الاستخبارات وغيرها من الأجهزة الحكومية الأخرى كالمباحث الفدرالية والقوات الجوية(www.nipc.gov).

وزادت بعد هجمات سبتمبر الشهيرة في الولايات المتحدة، دعوات البعض للقيام بأعمال إرهابية إلكترونية ضد مواقع عربية وإسلامية بحجة أنها تدعم الإرهاب، وهذا خبر أوردته شبكة (CNET)

الإخبارية تضمن اتفاق 60 خبيراً في أمن الشبكات للقيام بتلك الهجمات الإرهابية خاصة على مواقع فلسطينية وأفغانية.

ومن الجرائم الإرهابية المنتشرة تلك الجرائم التي ترتكبها عصابات المافيا المشهورة بالإجرام المنظم، التي أخذت بالوسائل التقنية الحديثة في تنظيم وتنفيذ أعمالها، فعملت على إنشاء مواقع خاصة بها على شبكة الإنترنت لمساعدتها في ادارة عملياتها وتلقي مراسلاتها واصطياد ضحاياها وتوسيع أعمالها وتسهيل عمليات غسيل الأموال، وتستخدمها أيضاً في إنشاء مواقع افتراضية تساعدها في تجاوز قوانين البلاد التي ترتكب فيها جرائمها، وهناك الكثير من المواقع التي يحتوي اسمها أو اسم نطاقها على كلمة مافيا، ومنها مواقع للمافيا اليهودية. ومن هذه المواقع ما هو مخصص للأعضاء فقط ولا يسمح لغيرهم بتصفحها، وهناك مواقع للعامة يمكن تصفحها (الجنبيهي منير والجنبيهي ممدوح، 2005، ص92-93).

بالتالي نلاحظ أن جرائم الإرهاب الإلكتروني والجريمة المنظمة قد استفادت كثيراً من التطور التكنولوجي، ووسائل الاتصال والتكنولوجيا والعولمة غير المقيدة بقيود الزمان والمكان، وقامت عصابات الإجرام المنظم باستخدام الامكانيات المتاحة في وسائل الإنترنت للتخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية.

وتتعدد صور الجرائم الإرهابية الإلكترونية[12]، فلا يشترط أن يكون الإرهاب الإلكتروني متخذاً لطابعاً أو نمطاً واحداً من أنماط السلوك أو النشاط الإجرامي، فقد يتكون من عدة جرائم، وكل جريمة تعد

---

12 سهل الانترنت ارتكاب جرائم تقليدية بطرق أكثر تعقيداً كالاحتيال، توزيع المواد الاباحية، وترويج الدعارة، وبيع الأسلحة، وتجارة المخدرات وبعض مظاهر الاجرام المنظم، والتوزيع غير المصرح به وغير القانوني لبرامج الحاسوب وغيره من مصنفات الملكية الفكرية (عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، **ص**29). فهناك الكثير من الجرائم التقليدية التي يمكن ارتكابها أو تسهيل ارتكابها من خلال الانترنت، ويطول شرح مثل هذه الجرائم وتقوم الباحثة في هذا المبحث بتناول بعض الجرائم الهامة. ومن الجرائم التي يمكن ان ترتكب من خلال الانترنت والتي لا تتطرق لها الباحثة في هذه الدراسة(سلامه، 2006، ص167):

1. تجارة المخدرات عبر الإنترنت: فهناك مواقع منتشرة على شبكة الإنترنت يتم من خلالها الترويج للمخدرات وكيفية استخدامها وكيفية زراعتها وصناعتها. كما يمكن ان يتم ذلك ليس من خلال المواقع فقط بل يمكن من خلال المنتديات

مستقلة بذاتها كجريمة عادية وليس إرهابية إلا أنها بارتباطها بعناصر الإرهاب وأساليبه وأهدافه وخطره والنتيجة الجرمية المبتغاة منها كما تم الوقوف عليها سابقاً فإنها تعد من الجرائم الإرهابية حينها. وفي هذا المبحث تحاول الباحثة توضيح مفاهيم تلك الجرائم التي تشكل بمفردها أحياناً أو باشتراكها كلها أو بعضها في تحقق جريمة الإرهاب الإلكتروني.

لذا فإن الباحثة تتناول هذه الجرائم كالاتي:

المطلب الاول: جرائم الاعتداء على الأشخاص والأموال

المطلب ثاني: جريمة الدخول غير المصرح به والعقاب عليها

المطلب الثالث: جرائم تساعد في تحقيق جرائم الإرهاب الإلكتروني أو ترافقها

وغرف الدردشة. بالمقابل تم إنشاء مواقع تحارب المخدرات وتساعد المدمنين على تجاوز محنتهم ومن ذلك الموقع الخاص بجماعة (Join-Together) وعنوانهم على النت هو http://192.12.191.21

2. الاحتيال الإلكتروني في: الاتصالات الهاتفية، وفي البريد الصوتي، وفي بطاقات الاتصال، وتليفونات الجوال والاحتيال بالهواتف المقلدة.

المطلب الاول: جرائم الاعتداء على الأشخاص والأموال

ونتناول هذا المطلب في فرعين:

الفرع الاول: جرائم الاعتداء على الأشخاص

الفرع الثاني: جرائم الاعتداء على الأموال

الفرع الاول: جرائم الاعتداء على الأشخاص

تتميز هذه الجرائم بوصفها جرائم عادية بصورتها الطبيعية، أم كانت من ضمن جرائم وأنشطة إرهابية، بأنها تقع أو تنصب على الانسان وكرامته وسمعته وحياته، ومن هذه الجرائم:

أولاً: الذم والقدح والتحقير

وهي الجرائم الأكثر شيوعاً والتي تمثل اعتداء على الشرف والاعتبار والكرامة من خلال الإنترنت، والتي قد تكون وجاهة أو غيابياً وقد تكون باللفظ أو بالكتابة وذلك حسب وسائل الاتصال المستخدمة، فقد تكون بالبريد الإلكتروني أو بشبكة الويب العالمية أو من خلال المجموعات الإخبارية، أو غرف المحادثة والدردشة وهي ما تعرف بالمراسلات الإلكترونية عبر طرفية إنترنت متصلة (الشوابكة، محمد، 2004، ص32-46). وقد تكون مراسلات إلكترونية عبر طرفية إنترنت غير متصلة كالرسائل القصيرة المستخدمة من خلال الهاتف النقال والاتصال بالبريد الإلكتروني وبالمواقع الأخرى من خلاله (سلامه، 2006، ص197-198).

ويمكن القول أنه من الصعوبة اعتبار أن هذه الجرائم قد ترقى إلى مستوى الجرائم الإرهابية، إلا أن الباحثة ترى أن من الممكن أن تصاحب هذه الجرائم الجرائم الإرهابية، أو قد تكون بذاتها أفعالاً تشكل أداة ارتكاب الجرائم الإرهابية، أو طريق لمباشرة النشاط المادي المكون للركن المادي للجريمة. ويجب

لاكتمال الجريمة حسب التشريع الأردني الذي يعاقب على القذف والسب أن تتم هذه الأعمال من خلال وسائل علانية، وقد نصت المادة 73 من قانون العقوبات على هذه الوسائل كالآتي:

أ. الأعمال والحركات إذا حصلت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو حصلت في مكان ليس من المحال المذكورة غير أنها جرت على صورة يستطيع معها أن يشاهدها أي شخص موجود في المحال المذكورة

ب. الكلام أو الصراخ سواء جهر بهما أو نقلا بالوسائل الآلية بحيث يسمعها في كلا الحالين من لا دخل له في الفعل.

ج. الكتابة والرسوم والصور اليدوية والشمسية والأفلام والشارات والتصاوير على اختلافها إذا عرضت في محل عام أو مكان مباح للجمهور، أو معرض للأنظار أو بيعت أو عرضت للبيع أو وزعت على أكثر من شخص

ثانياً: جرائم الاعتداء على حرمة الحياة الخاصة عبر الإنترنت

وتمثل المعلومات على الشبكة نوع من الملكية الخاصة لصاحبها لذا فإنها محمية بحماية الحق بالخصوصية لأنها تعرضت كثيراً للاعتداء من خلال بعض الممارسات على الشبكة منها بنوك المعلومات وجريمة التسجيل غير المشروع للبيانات الاسمية وجريمة الحفز غير المشروع للبيانات الاسمية وجريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية وجريمة الإفشاء غير المشروع للبيانات الإسمية (سلامه، 2006، ص184. وابراهيم، 2009، ص124-125).

وكما هو الحال في جرائم الذم والقدح فقد يكون من الصعوبة تصور علاقة بين الجرائم الإرهابية وبين هذه الجرائم، إلا أنه من الممكن أن تكون هذه الأفعال جزءً من مشروع إجرامي واحد يتضمن كثير من الأفعال، منها هذه الجرائم بوصفها مستقلة أو كجزء من النشاط المكون للركن المادي لجريمة الإرهاب.

ثالثاً: جرائم الاستغلال الجنسي للأطفال عبر الإنترنت [13]:

أشارت الباحثة إلى هذه الجريمة عند الحديث عن قانون جرائم أنظمة المعلومات المؤقت، حيث ورد تجريمها في المادة الثامنة والتاسعة منه، وفي هذا الصدد تتعرض الباحثة لهذه الجرائم ليس من باب خطة المشرع الأردني في التجريم، إنما من باب اعتبارها من الجرائم التي تصاحب الأعمال الإرهابية أو التي قد تكون جزء من مشروعها الإجرامي وركنها المادي الذي قد يتكون من عدة أفعال.

يتم استخدام الفضاء الإلكتروني في كافة المجالات ومن المظاهر غير الأخلاقية التي ظهرت في استخدام الفضاء الإلكتروني وتقنية المعلومات عرض الصور الخلاعية والإباحية المخلة بالآداب والأخلاق العامة. وهذه الصور موجهة لكافة الشرائح ويغدو الأكثر تأثيراً على شريحة الأطفال الذين يجب حمايتهم من هذه المواد الإباحية، وقد يقع هؤلاء الأطفال ضحايا لاعتداءات جنسية من خلال تصويرهم بأوضاع جنسية مخلة بالآداب وقد تقع على أطفال افتراضيين فيما يعرف بالصور الزائفة أو من خلال تركيب صور أطفال على أجساد عارية وفي أوضاع جنسية مخلة مما يشكل اعتداء على الطفولة وعلى الآداب والأخلاق العامة وعلى ملكية الشخص للصورة واستغلاله المادي لها (الشوابكة، محمد، 2004، ص105).

وتتمثل المخاوف وراء الأخطار المحتملة ضد الأطفال فيما يلي (Gina de Angelis، 2000 ، P50، من: الشوابكة، صالح، 2004، ص106):

أ. أن الأطفال قد يصلوا إلى مواقع خلاعية رئيسية تنظم دعارة الأطفال عبر شبكة الإنترنت ولهم القدرة في الوصول إلى ذلك من خلال محركات البحث ومواقع التصفح المختلفة.

ب. وجد منتجي دعارة الأطفال الإنترنت مكاناً مناسباً لبيع منتجاتهم من المواد والأفلام الخاصة بهذه الدعارة الأمر الذي يشكل تكريساً للانتهاك الجنسي للأطفال، إذ تشكل انتقالاً من الصور

---

13 للتعمق: سلامه، 2006، ص199-200.

الإباحية للبالغين إليهم، وقد انتشرت مبيعات أفلام الخلاعة عبر شبكة الإنترنت للبالغين علماً بأن هذه التجارة مشروعة في معظم قوانين الدول.

ت. وجود أشخاص خطرين منجذبين للأطفال علـــى شـــبكة الإنترنـــت يـــسحرون ضـــحاياهم ويستميلونهم إلى لقاءات حقيقية في الحياة من خلال مخاطبة البريـــد الإلكترونـــي وغـــرف المحادثة أو من خلال المراسلة عبر البريد الإلكتروني.

الفرع الثاني: جرائم الاعتداء على الأموال عبر الإنترنت

لم يقتصر أثر المعلوماتية على مجرد الاعتداء على الغير بل أن القدرة على معالجـــة البيانـــات ونقلها سواء في شكل خدمات أو منتجات مستحدثة منحها قيم تجارية ذات طابع مالي هيئ الفرصة لظهور قيم اقتصادية مستحدثة (الشوا، 1998، ص7).

فلم تقتصر أساليب إساءة استخدام الثورة التقنية على الاعتداء على الأشخاص إنما تعـــدت ذلـــك لتطال الذمم المالية للغير فقد تشمل اعتداء على الأموال المادية المحمية بالقانون وكذلك الأموال المنطقية أو المعنوية.

وفي مجال الإنترنت يغدو الأمر أكثر دقة وأهمية منه في مجال جرائم الحاسب الآلي الذي غالبـــاً ما يكون محلاً للجريمة والاعتداء باعتباره مالاً منقولاً أو قد يكون وسيلة لارتكاب جريمة، فـــالأمر هنـــا اعتداء على البرمجيات والتقنيات التي تستخدم لارتكاب جرائم على الغير أو قد تكون ذاتها محلاً للجريمة حيث ظهر ذلك في مجال جرائم الاعتداء على الأموال واتخذ عدة صور منها سرقة المـــال المعلومـــاتي وجريمة التحويل الإلكتروني غيرا لمشروع للأموال وجرم اتلاف النظم المعلوماتيـــة(ابـــراهيم، 2009، ص128-129).

وإن كانت هذه الجرائم تعد مشابهة للجرائم التقليدية ومن الظاهر أن لا علاقـــة لهـــا بالإرهـــاب الإلكتروني إلا أنه بإمعان النظر بهذه الجرائم نجد أنها ذات صلة وثيقة بجرائم الإرهاب الإلكتروني. لأن

الأموال قد تكون هدفاً للجريمة الإرهابية أي محلاً لها، وقد تكون جريمة مسهل لتحقيق وتنفيذ جريمة الإرهاب بشكل عام والإرهاب الإلكتروني بشكل خاص.

وهنا تتعرض الباحثة لبعض صور هذه الجرائم التي تمثل اعتداء على الأموال كالآتي:

أولاً: الاعتداء على المال المعلوماتي

أحياناً يتم استخدام مصطلح السرقة في غير المفهوم التقليدي لجريمة السرقة، وهناك من يحاول تكييف سرقة المال المعلوماتي في ظل إطار جريمة السرقة التقليدية، لكن الباحثة تعالج هذا الأمر مستخدمة هذا المصطلح مجازاً، حيث تقصد الباحثة من هذه الجرائم جرائم التقاط المعلومات، والتجسس، وبعض الأفعال التي تشكل اعتداء على المعلومات والتي يتشابه مع السرقة، وهناك ما يتعلق بسرقة المنفعة.

بالتالي فإن الاعتداء على المال المعلوماتي يعني ذلك اختلاس البيانات والمعلومات والاستفادة منها باستخدامها بشكل غير شرعي من خلال استخدام شخصية المجني عليه ليبدأ بها عمليات السرقة المتخفية عبر الإنترنت بحيث تؤدي بالغير إلى تقديم الأموال المادية والإلكترونية على السواء إلى الجاني عن طريق التحويلات البنكية(الشوابكة، محمد، 2004، ص138).

ويتم ارتكاب هذه الجريمة من خلال صورتين رئيسيتين هما:

1. الالتقاط غير المشروع للبيانات

ويتمثل ذلك بالدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن بشكل يتيح للمجرم المعلوماتي ممارسة نشاطاته الإجرامية لتحقيق مكاسب شخصية متباينة ومتعلقة بذات المجرم تمكنه من التقاط البيانات المخزنة في قواعد البيانات أو المتبادلة عبر قنوات الإنترنت واستخدامها بطرق غير مشروعة، ويتم التقاط هذه البيانات بعد الدخول غير المشروع إلى النظام من خلال التجسس الإلكتروني أو عن طريق الاحتيال أو الخداع أو عن طريق تفجير الموقع المستهدف(الشوابكة، محمد، 2004، ص166).

أ. التجسس الإلكتروني:

يتم ذلك من خلال قراصنة يستخدمون برامج تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الإنترنت كالمؤسسات والشركات التجارية ثم استخدام هذه المعلومات في ممارسة أنشطة جنائية(الصغير، 1999، ص36).

وبحجم خطورة المعلومات يكون حجم الخطر الناتج عبر التجسس الإلكتروني فقد تكون المعلومات شخصية وقد تكون اجتماعية وقد تكون ذات قيمة اقتصادية أو سياسية أو حربية أو عسكرية أو تتعلق ببطاقات ائتمان (الشوابكة، محمد، 2004، ص167) . ونتناول ما يتعلق بالاعتداء على المصالح العامة ضمن المطلب المتعلق بالجرائم التي ترافق جريمة الإرهاب الإلكتروني وتساعد في تحقيقها، والاكتفاء هنا بالتجسس المتعلق بالحياة الخاصة.

ب. أسلوب الخداع:

من خلال إنشاء مواقع وهمية خاصة من قبل قراصنة الإنترنت تتشابه مع المواقع الأصلية للشركات والمؤسسات التجارية المتعاملة بالتسويق عبر الإنترنت وغيرها من المواقع على الشبكة حيث يتم استقبال جميع المعاملات التجارية والمالية ومن ضمنها المعلومات والبيانات الخاصة والسرية كمعلومات بطاقات الائتمان والدفع الإلكتروني(جميل عبد الباقي الصغير، 1999، ص37).

ج. تفجير الموقع المستهدف:

يعني ذلك ضخ كميات كبيرة من الرسائل الإلكترونية من جهاز الحاسب الآلي للجاني، يؤدي بالمحصلة إلى تفجير الموقع العامل على الشبكة فتشتت المعلومات والبيانات المخزنة فيه لتنقل بعد ذلك إلى الجهاز الخاص بالمجرم أو تمكنه من حرية التجول في الموضع المستهدف بسهولة والحصول على كل ما يحتاجه خاصة الأرقام والمعلومات (حجازي، عبدالفتاح، النظام القانوني لحماية التجارة الإلكترونية، 2002، ص132).

2. سرقة منفعة الحاسب الآلي:

أي استخدامه لأغراض شخصية أو تجارية بدون علم مالك الحاسب أو حائزه القـانوني، وهـذا بالطبع يستتبع استخدام وقت الحاسب الآلي لأغراض شخصية وهذا بالتأكيد يخلق طائفة جديدة من الجرائم المعلوماتية تتمثل بسرقة وقت الحاسب الآلي، وقد تكون هذه الأفعال لغايات خيرية أو غير خيرية(الشوا، 1999، ص220).

وتتم سرقة منفعة الحاسب من خلال الدخول غير المشروع للأنظمة المعلوماتية لسرقة الخـدمات المعلوماتية أو سرقة وقت الحاسب الآلي ومنفعته. وتعد هذه الجريم أساساً جريمة سرقة، وقد حاول الكثير تكييفها في هذا الإطار من باب وضع حد للنشاط الإجرامي في مجال الحاسب الالي والإنترنـت التـي تتعلق بالاستيلاء على المعطيات.

فالسرقة هي:

- اعتداء على حق الملكية وفي مجال الحاسب الالي والإنترنت يمكن تملك البيانات والمعلومات
- وهي اعتداء على الحيازة أساساً لامكان الاعتداء على الملكية
- وموضوعها **المال المنقول** وفق القانون الأردني

- ومحلها شيء مادي وهذا ما هو ممكن في بيئة الحاسب الالي والإنترنت. ويوجد مايشبه ذلك في بعض التشريعات كما هو الحال بالنسبة للكهرباء والقوى المحرزة في قانون العقوبات الأردني. حيث تعرف جريمة السرقة أنها: "اعتداء على ملكية منقول وحيازته بنية تملكه" (حسني، 1988، ص88). وقد عرفها قانون العقوبات الأردني في المادة (1/399) بأنها " أخذ مال الغير المنقول دون رضاه " وحدد المراد بأخذ المال بأنه " إزالة تصرف المالك فيه برفعه من مكانه ونقله ، واذا كان متـصلاً بغيـر منقـول فبفصله عنه فصلاً تاماً ونقله " (م 2/399) وقرر أن لفظه مال تشمل القوى المحرزة (م 3/399).

ومن صور الاستيلاء على معطيات الحاسوب (عرب، صور الجـرائم الإلكترونيـة واتجاهـات تبويبها، 2006، ص16):

أ. الالتقاط الذهني للبيانات إثر مطالعتها بالبصر، أو سماعها بالاذن، ثم العمل علـى اختزانهـا، أو حفظها بشكل واعي أو عرضي.

ب. النسخ غير المشروع للبيانات المخزنة إلكترونياً بطريق التعامل المباشر مع نظام الحاسوب أو عن طريق التوصل غير المرخص به مع نظام الحاسوب.

ت. اعتراض معطيات الحاسوب خلال نقلها، والتقاطها بواسطة احـدى الطـرق التقنيـة للالتقـاط واعتراض الرسائل والبيانات.

ثانياً: التحويل الإلكتروني غير المشروع للأموال

ساهمت المعلوماتية بازدياد نشاط الحركات التجارية والمعاملات المالية حيث أصـبح بالإمكـان تحويل الأموال من خلال البيوت والمكاتب وفي مختلف أنحاء العالم ورافق ذلك خطـورة ناجمـة عـن إمكانية التلاعب بالبيانات والمعلومات وإجراء تحويلات غير مشروعة من خلال الدخول غير المـشروع لمخترقي شبكات الإنترنت إلى حسابات الآخرين والحصول على كلمات المرور واستخدامها، حيـث تـم الحصول عليها بالالتقاط أثناء التواجد في النظام المعلوماتي أو من خلال بث بـرامج تتعقـب الأنظمـة المعلوماتية التي يتجه إليها أكثر المستخدمين وسرقة كلمات المرور الخاصة بهم والحصول على البيانات الخاصة بالجاني واستخدام المفيد منها في إجراء التحويلات الإلكترونية للأموال من حساب المجني عليه وإدخالها في الأرصدة الخاصة بالجناة (الشوابكة، محمد، 2004، ص178).

وقد سبقت الإشارة إلى هذه الجريمة في ظل قانون جرائم أنظمة المعلومات الأردني المؤقت لعام 2010، وقد تعرضت الباحثة لهذه الجريمة في هذا الصدد، من باب التعريف بأدوات ارتكـاب جريمـة الإرهاب الإلكتروني ووسائلها.

ثالثاً: جريمة إتلاف نظم المعلوماتية عبر الإنترنت

وردت هذه الجريمة في المادة الثالثة والرابعة والخامسة من قانون جرائم أنظمة المعلومات الأردني المؤقت، وقد تطرقت لها الباحثة، ويتمثل السوك الجرمي أو الركن المادي في الاتلاف بادخال غير مشروع للبيانات. أو محو المعلومات. أو تعديل المعلومات. ويقصد باتلاف النظم المعلوماتية تدمير المعطيات التقنية وليس المواد أو الدعامات التي تتواجد عليها لأن هذه الحالة تتفق مع الأحكام العامة في الجرائم لأنها اعتداء على كيانات مادية. بالتالي فإننا نعني بذلك الاعتداء على البيانات والمعطيات المنطقية، بشكل يؤدي إلى محو كلي أو جزئي لها يمنع من إمكانية استخدام النظام بشكل طبيعي.

ويمكن ظهور التخريب بشكل واضح وجلي كما هو في البنية التقليدية حيث يمكن استهداف نظم الاتصال وخدماته لتخريبها وتحقيق أهداف معينة ومن الأدوات المستخدمة في التخريب: التشويش، قنابل تحويل النبضات الكهرومغناطيسية، البنادق، أسلحة ترددات الراديو، أسلحة الموجات الضيقة (البداينة، 2002، ص295-298). اما الأساليب الفنية للاتلاف فهي: فيروسات الحاسب الالي، برامج الدودة، والقنابل المعلوماتية (ميلاد، 2007، ص93-94، وص97).

ويتمثل جوهر هذه الجريمة في تخريب الشيء محل الاتلاف أو الانتقاص من منفعته وجعله غير صالح للاستعمال أو تعطيله (قشقوش، 1993، ص564.). وقد يكون ذلك على الأشياء المادية واللامادية أو المعنوية على السواء أي الاعتداء على الشبكة وعلى سير نظام المعالجة الآلية للبيانات كالدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه وإتلاف البيانات والبرامج بشكل يؤدي إلى تعطيله، أو إفساد نظام التشغيل.

وتقوم هذه الجريمة على أفعال وتعتدي على الوظائف الطبيعية للحاسب الآلي كالبرامج والبيانات المخزنة والمتبادلة على الشبكة الداخلية أو العالمية من خلال التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو من خلال إتلاف المعلومات المخزنة بالحواسب والمتبادلة عبر الشبكة العالمية لمحوها أو تعديلها أو تغيير نتائجها أو بطريق التشويش على النظام المعلوماتي بشكل يؤدي إلى عرقلة سير عمل

النظام الآلي واختلال وظائفه، ويكون الاتلاف المقصود للبرامج والبيانات بمحوها أو تدميرها أو تشويهها كلياً أو جزئياً (قشقوش، 1993، ص553. والرومي، 2003، ص56)[14].

ومن أمثلة هذه الجريمة، والتي يتضح منها أيضاً ارتباط الإرهاب أحياناً بالجرائم الاقتصادية، حيث يتم الدخول إلى الشبكة لارتكاب جرائم اقتصادية ذات أثر وطابع إرهابي، لارتكاب الجرائم الاقتصادية، خاصة مع تحول كثير من الدول إلى الحكومات الإلكترونية، ففي مثل هذه الدول استفاد المجرمون من التقدم التقني في ارتكاب جرائم اختلاس الأموال، وجرائم تحويل الارصدة النقدية، وجرائم سرقة خطوط الهاتف والعبث بها واتلافها.

ومن هذه الهجمات تلك الهجمات التي تقع على شبكات الطاقة الكهربائية، حيث أصبحت هذه الشبكات تعتمد على شبكات المعلومات لإدارة نظم الطاقة الكهربائية، وتؤدي هذه الهجمات إلى نتائج خطرة وحقيقية، لذا فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من أهداف الإرهاب الإلكتروني.

وقد وقعت حادثة تمثلت باقتحام متسللين لنظام الحاسب الآلي الذي يتحكم بتدفق أغلب الكهرباء في مختلف أنحاء ولاية كاليفورنيا الامريكية، وبالرغم من أن الهجوم كان محدوداً، إلا أنه كشف عن ثغرات أمنية في نظام الحاسب الآلي لشركة الكهرباء. ومن الهجمات على الأهداف الاقتصادية ما قامت بها مجموعة هكرة نادي الفوضى عام 1997، حيث قامت المجموعة بإنشاء برنامج تحكم بلغة آكتف إكس مصمم للعمل عبر الإنترنت ويمكنه خداع برنامج كويكن Quicken المحاسبي، حيث يقوم بتحويل

---

14 وتهدف هذه الهجمات إلى تعطيل النظام وتحويله إلى عاجز عن العمل، وقد تستخدم لأغراض تخريبية وإرهابية، ومن الأهداف والأنشطة التي تتضمنها: إثارة الأحقاد، والإساءة للأفراد، والتحرش بهم، ومضايقتهم، وابتزازهم عبر الرسائل الإلكترونية، ونسبة الإساءات إلى أشخاص آخرين، لا علم لهم بها، باستغلال اسمهم أو عناوينهم الإلكترونية، وأنشطة مواقع الحوار غير القانونية، وإرسال رسائل دعائية بالبريد الإلكتروني دون طلب، وبشكل يزعج المتلقين، ونشر المواد الإباحية، وإدارة أنشطة المقامرة، والقيام بأنشطة الغسيل الإلكتروني للأموال، وظاهرة الإرهاب الإلكتروني، واستغلال الإنترنت للوصول إلى النظم والشبكات المحلية، لإلحاق الاذى والخوف والتهديد بأفراد المجتع ومؤسساته الحيوية (عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، ، 2006، ص28).

الأموال من الحساب المصرفي للمستخدمين، ويمكن الهكرة من سرقة الأموال من أرصـــدة مـــستخدمي برنامج كويكن في جميع أنحاء العالم(داود، 2000، ص45−47).

وتتم عملية الاتلاف هذه باحدى صورتين (يونس عرب، صور الجرائم الإلكترونيـــة واتجاهـــات تبويبها، 2006، ص25):

أ. محو أو تشويه البيانات المخزنة في نظم الحواسيب من خلال التوصل غير المرخص به مع النظام، وهذه الطريقة تعد اقل خطورة من الوسيلة الثانية.

ب. نشر البرامج الخبيثة والضارة كالفيروسات والديدان والقنابل المنطقية و الموقوتة.

أما بالنسبة لأركان جريمة اتلاف المعطيات فهي:

أ. الركن المادي أي فعل الاتلاف كتخريب المال أو اتلافه أو جعله غير صالح للاستعمال أو تعطيله، وينصب ذلك على الأموال المنقولة وغير المنقولة المملوكة للغير.

ويتطلب الركن المادي توافر عنصر النتيجة، إذ أن فعل الاتلاف يعد من الجرائم المادية التي تتطلب تحقق نتيجة، وتتمثل نتيجتها باتلاف المال باحدى صور الاتلاف بشكل يلحق ضرراً بالغير.

ب. الركن المعنوي: وهو القصد الجنائي العام المتكون من عنصري العلم والإرادة، ويتمثل بنية الجاني ارتكاب فعل الاتلاف رغم نهي القانون عنه، واتجاه ارادته إلى النشاط والنتيجة.

وقد أخذ القضاء الانجليزي في قضية (Cox. V. Rily) وقضية (Her Majesty. V. Wilson) بالادانة على أفعال الإضرار بالبرامج والبيانات، وبالرغم من تعرض هذا الحكم للنقد، فإنه وبصدور قانون اساءة استخدام الحاسوب لسنة 1990 قضت محكمة الاستئناف في تطبيق لهذا القانون عام 1991 بصراحة بتطبيق أحكام بعض الجرائم التقليدية حيثما يقع الضرر أو الاعتداء على بيانات الحاسوب (عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص26).

ومن القوانين المقارنة التي جرمت الإتلاف الإلكتروني (يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص27):

- القانون الفدرالي الأمريكي بشأن غش وإساءة استخدام الحاسوب لسنة 1984 في المـــــادة 1030 / أ / 3.
- القانون المعدل لقانون العقوبات الكندي لعام 1985 (المادة 387 منه تعاقب كل من يقوم عن عمد ودون مبرر قانوني أو عذر باتلاف أو تشويه البيانات أو محوها أو جعل البيانات بلا معنى أو بدون فائدة أو غير مؤثرة أو فعالة أو باعاقة أو مقاطعة الاستخدام المشروع للبيانات أو منع من له الحق في الوصول إلى البيانات من الوصول اليها.
- كذلك عاقب المشرع الالماني في المادة 303 من قانون العقوبات المعدلة بموجب القانون الثاني لمكافحة الجريمة الاقتصادية عام 1986 كل من محا أو أبطل أو جعل غير نافع أو أحدث تغييراً في البيانات بصور غير مشروعة، بالحبس لمدة لا تزيد على عامين أو الغرامة، وشدد العقوبة لتصل إلى خمس سنوات أو الغرامة إذا ارتكبت هذه الأفعال على بيانات ذات أهمية أساسية لقطاع الأعمال أو السلطات الادارية، أو في الحالات التي تؤدي هذه الأفعال إلى تدمير أو اتلاف أو ازالة أو تعديل نظام حاسوب أو دعامة بيانات أو جعلها غير مفيدة.

- جرم المشرع الفرنسي في قانون 1988 محو وتعديل البيانات المعالجة آلياً أو التـــدخل فـــي طـــرق معالجتها (م 4/462) وعاقب عليه بالحبس مدة تتراوح بين ثلاثة أشهر وثلاث سنوات أو بالغرامة. كما جرم تعطيل أو افساد (عن عمد) تشغيل نظام المعالجة الالية للبيانات وعاقب عليه بذات العقوبة المشار اليها (م 3/462).

أما بالنسبة لموقف المشرع الأردني من جريمة الاتلاف الإلكترونـــي الـــذي يـــوازي الإرهـــاب الإلكتروني في بعض الحالات، فلا يوجد ما يتعلق بذلك في قانون العقوبات الأردني، وقبل صدور قانون

جرائم أنظمة المعلومات كان جانب من الفقه يميل إلى تطبيق النصوص التقليدية المتعلقة بالاتلاف أو الإضرار الواقع على المال، ومن هنا حاول هذا الاتجاه تطبيق شروط المال وصفاته على المعلومات من حيث عدم اشتراط الصفة المادية في محل الجريمة، وإمكانية اعتبار المعلومات كياناً مادياً تبعاً للقيمة الاقتصادية لها (ميلاد، 2007، ص51-54). وقد كان هناك بعض الأحكام والامكانية في القوانين الخاصة من خلال ما يأتي:

أ. قانون المعاملات الإلكترونية، والذي يتبنى العقوبات الواردة في التشريعات الأخرى من خلال نص المادة 38 منه، والتي تفيد بأنه:"يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة أو بغرامة لا تقل عن (3000) ثلاثة الاف دينار ولا تزيد على (10000) عشرة الاف دينار أو بكلتا هاتين العقوبتين ، ويعاقب بالعقوبة الاشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون".

بالتالي يمكن تطبيق هذه المادة بالتوافق مع الفقرة الأولى من المادة 445 من قانون العقوبات الأردني التي تتعلق بالأضرار بمال الغير والتي تفيد بأنه:"كل من ألحق باختياره ضرراً بمال غيره المنقول يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين".

ب. قانون الاتصالات الأردني لسنة 1995

عاقب المشرع الأردني على الإتلاف المادي لمنشآت الاتصالات وإتلاف أدوات الحاسب الإلكتروني وشبكاته بشكل يؤثر على برامجه وبياناته أو على سير عمل النظام المعلوماتي من خلال قانون الاتصالات رقم 13 لسنة 1995 حيث نصت المادة 72 منه على أنه:"أ. كل من أقدم قصداً على تخريب منشآت الاتصالات أو ألحق بها ضرراً عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل على (200) دينار ولا تزيد على (5000) دينار أو بكلتا العقوبتين ، وتضاعف العقوبة إذا تسبب فعله بتعطيل حركة الاتصالات.

ب .كل من تسبب إهمالاً في تخريب منشآت الاتصالات أو إلحاق الضرر بها يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على (100) دينار أو بكلتا العقوبتين".

والمادة 76 التي تنص على أنه:" كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين ".

ج. قانون حماية حق المؤلف لسنة 1992

حيث عاقب المشرع على مثل هذا الاتلاف من خلال المواد الآتية:

- المادة 54 – التي أضيفت بالقانون رقم 9 لسنة 2002– والتي تنص على:" يعتبر مخالفاً لأحكام هذا القانون كل من قام بأي من الأفعال التالية : 1– حذف أو غير أي معلومات واردة في شكل إلكتروني دون اذن صاحب الحق فيها لضمان إدارة الحقوق. 2– وزع أو استورد لأغراض التوزيع أو اذاع أو نقل إلى الجمهور دون إذن نسخاً من مصنفات أو اداءات مثبتة أو تسجيلات صوتية مع علمه أو إذا توافرت الأسباب والقرائن الكافية للعلم".

- الفقرة أ من المادة 55 والتي تفيد بأنه يعتبر مخالفاً لأحكام القانون كل من قام بأي من الأفعال التالية:1– تحايل على التدابير التكنولوجية الفعالة أو أبطل أو عطل أياً منها. 2– صنع أو استورد أو باع أو عرض لغايات البيع أو التأجير أو حاز لأي غاية تجارية أخرى أو وزع أو قام بأعمال دعائية للبيع والتأجير لأي قطعة أو جهاز أو خدمة أو وسيلة تم تصميمها أو انتاجها أو استعمالها لغايات التحايل على التدابير التكنولوجية الفعالة أو ابطال أو تعطيل أي منها.

لكن بصدور قانون جرائم أنظمة المعلومات الأردني المؤقت لعام 2010 لم يعد هناك حاجة لمثل هذه التكييفات، وقد نص المشرع الأردني صراحة ولأول مرة على هذه الجرائم بوصفها المستقل في

المادة الثالثة والرابعة منه، وقد تطرقت الباحثة كما أشارت مسبقاً لهذه الصورة من الجريمة هنا، ليس لغايتها ذاتها، إنما كوسيلة أو أداة لارتكاب جريمة الإرهاب الإلكتروني.

المطلب ثاني: جريمة الدخول غير المصرح به والعقاب عليها

عالج المشرع الأردني هذه الجرائم -كما سبق وأن أشارت الباحثة- في قانون جرائم أنظمة المعلومات الأردني المؤقت لعام 2010، وبذلك حسم المشرع الجدل الذي كان دائراً حولها، فأصبحت هذه الأفعال بموجب المادة الثالثة والمادة 11 منه تشكل جريمة مستقلة بذاتها، وهذه الجريمة قد تصاحب القيام بجريمة الإرهاب الإلكترونية وركنها المادي، وقد تكون وسيلة مساعدة لتنفيذ تلك الجريمة. فالإرهاب في الفضاء الإلكتروني يمثل مجموعة من الجرائم أيضاً فهو لا يصدق عليه وصف الفعل الواحد بل قد تتعدد الأعمال الإرهابية فقد تكون اعتداء على الأشخاص باستخدام الإنترنت لتسهيل ارتكاب أي جريمة فيها عنصر التخويف والذعر لدى الناس بما في ذلك أي جريمة من جرائم الاعتداء على الأشخاص عبر الإنترنت حتى وأن كانت جرائم القذف والسب متى دخلت ضمن إطار الأعمال الإرهابي، وقد تمثل الأعمال الإرهابية اعتداء على الأموال عبر الإنترنت كالسرقة وإتلاف النظم والتحويل غير المشروع للأموال عبر الإنترنت.

ومن أكثر جرائم الإنترنت انتشاراً وارتباطاً بالإرهاب الإلكتروني هو مسألة انتهاك الخصوصية حتى أن هذا الفعل ينتشر سواء ارتكب بوسيلة تكنولوجية أم تقليدية، ويعد هذا الفعل أمراً مجرماً وتكاد تجتمع أغلب التشريعات على ذلك ويعد بالتالي التطفل على المعلومات التي تمثل خصوصية ما سواء أكانت مخزنة في جهاز الحاسب الآلي أو في البريد الالتكروني أو في أي مكان آخر انتهاكاً لخصوصية الفرد، وقد ساهم انتشار الإنترنت في تعريض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية عمداً أو مصادفة، ويتم انتهاك الخصوصية عندما يزور مستخدم الإنترنت أي موقع على الشبكة فيقوم ذلك الموقع باصدار نسختين من الكعكة الخاصة بأجهزتهم (Cookies) وهي عبارة عن نصوص صغيرة ترسلها مواقع الويب لتخزينها في جهاز الزائر لعدة أسباب منها التعرف على من يكرر الزيارة للموقع أو لأية أسباب أخرى، وتبقى واحدة من هذه الكعكات في الخادم أو السيرفر الخاص بهم، وأخرى يتم تخزينها على القرص الصلب لجهاز الزائر في أحد الملفات التي قامت المواقع الأخرى بتخزينها من قبل، دون أن يشعر صاحب الجهاز الزائر بذلك، أو بدون استئذانه، ويتم تبعاً لذلك اصدار رقم خاص لذلك الزائر يميزه عن غيره من الزوار، ثم تبدأ الكعكة بأداء مهمتها بجمع المعلومات وارسالها إلى مصدرها، أو إلى إحدى

شركات الجمع والتحليل للمعلومات، وكلما قام الزائر بزيارة الموقع مرات أخرى، يتم ارسال المعلومات وتجديد نسخة الكعكة الموجودة لديهم، ويقوم متصفح جهاز الزائر بعمل ذات المهمة، مالم يقم صاحب الجهاز الزائر بتعديل وضعها. ويحصل أصحاب المواقع هذه على معلومات شخصية عن صاحب الجهاز. وقد تستغل بعض المواقع المشبوهة هذه الكعكات لتعمل على نسخ الملفات المجمعة من جهاز الضحية، والاستفادة منها بطريقة أو بأخرى (داود، 2000، ص50–52) .

يعد فعل الدخول غير المسموح به من حيث الصلاحية أو السلطة أو القانون وبنية الخرق أو السلب لحرمة الحاسب لسرقة كلمات الدخول أو أي رموز أخرى جريمة يعاقب عليها القانون في أغلب الدول، فهي تستهدف الوصول إلى حسابات على النظام من قبل متطفلين للحصول على معلومات معينة واستهداف أنظمة الحواسيب (سلامه، 2006، ص114. و البداينة، 2002، ص290–294).

وتعد هذه الجريمة من أكثر الجرائم الإلكترونية انتشاراً وتقوم أساساً على الدخول إلى نظام الحاسوب أو شبكة المعلومات من خلال استخدام وسيلة اتصال عن بعد كـ (المـوديم)، أو من خلال التوصل عبر نقاط الاتصال والموجهات الموجودة على الشبكة للدخول إلى نظام كمبيوتر معين، بغرض التواصل مع البيانات أو البرامج المخزنة في النظام. وتتطلب هذه الجريمة غالباً تجاوز أو كسر إجراءات الحماية التقنية للنظام، كتجاوز كلمة السر، وإجراءات التعريف، والجدران النارية وغيرها، أو التوصل لنقطة ضعف في نظام حماية البرامج، والنفاذ منها. وتتعدد أهداف الدخول فقد تكون عملية الدخول مجردة عن أغراض لاحقة، وقد لا تهدف إلى الإضرار بالبيانات والملفات أو تدميرها، وقد تهدف إلى الاطلاع على المعلومات المحمية، وقد تتطور الأهداف من مجرد هدف الاطلاع إلى أهداف أكثر خطورة كالتلاعب بالمعطيات أو اتلافها أو ارتكاب جرائم معينة أو استخدام الدخول لارتكاب جرائم أخرى بواسطة الكمبيوتر. وفعلياً يعد الدخول غير المصرح به الفعل الأول من بين أنشطة جرائم الكمبيوتر والإنترنت، فكل جريمة لابد وأن تبدأ بدخول غير مشروع فاما يستمر وإما أن يتوقف النشاط عند حد الدخول (عرب، 2006، ص14).

وقد أثارت عملية تجريم الدخول الممهد لجريمة أخرى جدلاً في الاوساط الفقهية. ويستقر جانب من الفقه على اعتبار أن الدخول الممهد لجريمة أخرى يقع في باب التعدد في الجرائم، فان استمر النشاط وتم ارتكاب فعلاً آخراً يؤخذ بالعقوبة الأشد، وأن توقفت عند حد الدخول فإنه يعاقب عليه (عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص14-15).

وفي الولايات المتحدة -الأكثر تطوراً في هذا المجال- فإن المعلومات وأنظمتها محمية تشريعياً، فقد جرم المشرع الفيدرالي فعل الدخول غير المشروع إلى النظام المعلوماتي في قانون الاحتيال وإساءة استخدام الكمبيوتر(CFAA) لعام 1996. فيعاقب التشريع الامريكي من يدخل عمداً إلى جهاز حاسوب بدون تصريح أو يتجاوز حدود التصريح الممنوحة له وكل من يصل عمداً إلى حاسوب بدون ترخيص أو يتجاوز حدود الترخيص الممنوحة له للحصول على معلومات محمية وكل من يصل عمداً بدون ترخيص ل أي حاسوب غير عام يخص إحدى إدارات أو وكالات الولايات المتحدة إذا كان مخصصاً بشكل وحيد لاستعمال الحكومة أو كان قد استعمل من قبل لأجل الحكومة، وكل من يصل عن معرفة وبقصد الغش إلى حاسوب محمي بدون ترخيص أو يتجاوز حدود الترخيص الممنوح له أو أي وسيلة تسهل الغش ويحصل على شيء ذا قيمة، وكل من يسبب عن معرفة ضرراً لبث برنامج أو معلومات أو شيفرة أو أمر لكمبيوتر محمي وبدون ترخيص أو يصل إلى كمبيوتر محمي بدون ترخيص أو تفويض، وكل من يسلب باحتيال عن قصد وعلم تجارة أو مقايضة بدون تفويض إذا كانت هذه التجارة تؤثر على الولايات المتحدة أو كان الكمبيوتر مستخدماً من قبل أو لأجل حكومة الولايات المتحدة، وكل من يقصد ابتزاز أي نقود أو أي شيء آخر ذا قيمة من أي شخص أو شركة أو جمعية أو هيئة حكومية أو أي كيان قانوني آخر(المادة 1030، الشوابكة، محمد، 2004، ص19).

المطلب الثالث: جرائم تساعد في تحقيق جرائم الإرهاب الإلكتروني أو ترافقها

في هذا المطلب تتناول الباحثة بعض أنماط الجرائم التي تعد جرائم مستقلة بذاتها، وقد تكون جزءً من مجموعة من الجرائم الداخلة في نطاق الإرهاب الإلكتروني. أو على الأقل قد ترافق الجرائم الإرهابية سواء التقليدية أم الإلكترونية. وتتناول الباحثة بالدراسة ما يرتبط فعلاً منها وبشكل أساسي بالإرهاب بصفة عامة، وبالإرهاب الإلكتروني بصفة خاصة، وهذه الجرائم هي جريمة غسيل الأموال الإلكتروني والتجسس الإلكتروني. وذلك من خلال الفروع الاتية:

الفرع الأول: جريمة غسيل الأموال إلكترونياً

تعددت التعريفات التي تناولت غسيل الأموال منها أنه:" أي عملية من شأنها اخفاء المصدر غير المشروع الذي اكتسبت منه الأموال" وقد استغلت طرق غسيل الأموال عصر التقنية واستخدمت الإنترنت لتوسعة وتسريع أعمالها وعلى الإنترنت مواقع متعددة تتعلق بغسيل الأموال[15](سلامه، 2006، ص201-202).

وبموجب تعليمات مكافحة غسيل الأموال الأردنية رقم 10 لسنة 2001 عرفت جريمة غسيل الأموال في البند الأول منها أنها: إخفاء المصدر الحقيقي للأموال غير المشروعة (المتأتية من عمل غير مشروع) أو إعطاء معلومات مغلوطة عن هذا المصدر بأي وسيلة كانت وتحويل الأموال أو استبدالها لغرض إخفاء أو تمويه مصدره. تملك الأموال غير المشروعة أو حيازتها أو استخدامها أو توظيفها بأي وسيلة من الوسائل لشراء أموال منقولة أو غير منقولة أو للقيام بعمليات مالية.

ويعرف غسيل الأموال فقهياً أنه إخفاء حقيقة الأموال المستمدة عن طريق غير مشروع بالقيام بتصديرها أو ايداعها في مصارف دول أخرى أو نقلها أو تحويلها أو توظيفها أو استثمارها في أنشطة مشروعة للافلات بها من القيود والمصادرة واظهارها كما لو كانت مستمدة من مصادر مشروعة سواء

15 منها الموقع: http://www.laundryman.u.net.com

أكان الايداع أم النقل أم التحويل أم التوظيف أم الاستثمار قد تم في دولة متقدمة أم في دولة نامية (عوض، 1998، ص22).

وعرفت هذه الجريمة بموجب دليل اللجنة الاوروبية لغسيل الأموال الصادر لعام 1990 أنها:"عملية تحويل الأموال المتحصلة من أنشطة جرمية بهدف إخفاء أو إنكار المصدر غير الشرعي والمحظور لهذه الأموال أو مساعدة أي شخص ارتكب جرماً ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم". ومن التعريف يتضح أن الأموال متحصلة عن جريمة جنائية كالمخدرات والإرهاب والفساد (سلامه، 2006، 202-205).

وتعد هذه الجرائم من أخطر جرائم عصر الاقتصاد الرقمي وتأتي غالباً كجريمة لاحقة لأنشطة جرمية أخرى حققت عوائد مالية غير مشروعة، لإضفاء المشروعية على تلك العائدات ليتم استخدامها بشكل طبيعي، كحالات الاتجار بالمخدرات وتهريب الأسلحة والاتجار بالرقيق والاختلاس. واكثر ما ترتبط هذه الجريمة بجرائم المخدرات حتى أن الجهود الدولية لمكافحة غسيل الأموال جاءت ضمن الجهود الدولية لمكافحة المخدرات، وذلك ضمن اتفاقية الأمم المتحدة المتعلقة بمكافحة المخدرات(الجنبيهي منير والجنبيهي ممدوح، 2005، ص99-100). وفي مجال مكافحة الإرهاب أيضاً يشهد العالم الآن حملة لمكافحة الإرهاب ترتبط بشكل أساسي بتجفيف منابع الإرهاب والمنظمات الإرهابية، وملاحقة أنشطتها الرامية لإخفاء مصادر تمويلها، الأمر الذي استدعى اعادة النظر في التشريعات التي تتعامل مع الإرهاب وتشريعات غسيل الأموال في مختلف دول العالم (يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص30)[16].

---

16 من أهم قضايا غسيل الأموال التي شهدها العالم قضية لوزارينكو (رئيس الوزراء الاوكراني السابق)، وتتمثل تفاصيل هذه القضية في أنه:"تمت ادانته بأنشطة غسيل الأموال من قبل القضاء السويسري، وفي الوقت ذاته وبعد هربه إلى أمريكا ومحاولاته اللجوء السياسي للتملص من الحكم السويسري الصادر بحقه، جرى توجيه الاتهامات اليه وتجري محاكمته أمام القضاء الأمريكي. وكان قد أدين لوزارينكو من قبل القضاء السويسري بتاريخ 2000/6/29 بالحبس لمدة 18 شهرا لقيامه بأنشطة غسيل أموال تبلغ 880 مليون دولار في الفترة ما بين 94 – 97 ، من بينها 170 مليون تم غسيلها عبر حسابات سويسرية، أما لوزارينكو فقد اعترف بعملية غسل 9 ملايين فقط، وقد تم اعتقال لوزارينكو من قبل السلطات السويسرية في كانون الثاني عام 1998 عندما دخل سويسرا

تتجه انشطة غسيل الأموال إلى استخدام الوسائل الإلكترونية لدخول الخدمات المالية الإلكترونية في أعمال البنوك، كخدمات البنوك الإلكترونية، وبنوك الويب، وعمليات الدفع النقدي الإلكتروني. كما أن من أهم انشطة غسيل الأموال إنشاء المشروعات الوهمية التي تستغل كواجهة لاخفاء مصادر الأموال، ويعد الإنترنت البيئة الاكثر مناسبة لإنشاء مثل هذه المشاريع (بن يونس، 2004، ص664).

وعرف الفقه غسيل الأموال الإلكتروني أنه مجموعة العمليات المالية الإلكترونية المتداخلة والتي تتم عبر الشبكة بغية اخفاء المصدر غير المشروع لتلك الأموال واظهارها في صورة أموال مشروعة، ومن أهم أنماط تلك الجريمة استغلال التحويل الإلكتروني عبر الإنترنت واستخدام بنوك الإنترنت في ايواء الأموال موضوع الغسيل واستثمار التجارة الإلكترونية في عمليا غسيل الأموال(الخييلي، 2006، 64).

بجواز سفر بنمي (بنما) مزور، واطلق سراحه بالكفالة البالغة 3 ميلون دولار امريكي ، وما لبث ان غادر إلى الولايات المتحدة في عملية لجوء سياسي في نيسان عام 1990، بعد أن تم ضبطه من قبل دائرة الهجرة في نيويورك لخرقه نظام الهجرة والفيزا ودخوله غير المشروع، وبناء على طلب أمريكي، قامت السلطات السويسرية بتجميد ارصدة 20 حساب بنكي يعتقد أنها تعود إلى لوزارينكو، وتم القاء القبض عليه واحتجازه ومنع كفالته نيابة عن السلطات السويسرية، ولم يلبث أن تقدم المدعي العام في سان فرانسيسكو بلائحة اتهام ضد لوزارينكو وشخص آخر هو بيتر كيرتشينكو الذي يعتقد بأنه هو الذي قام بتنفيذ عمليات غسيل الأموال، وتتضمن اللائحة اتهامهما بتحويل 114 مليون دولار أمريكي إلى (البنك التجاري في سان فرانسيسكو، والباسفيك بنك، ووست أميركا بنك، وبنك أوف أميركا، وميرل لينش، ولمؤسسة افليت بوستن روبيرتسون) خلال الأعوام من 94 -99، ولم يتم توجيه الاتهام إلى أي من هذه المؤسسات، إضافة إلى توجيه الاتهام لهما بشراء موجودات ومشاريع في أمريكا خلال عامي 97 - 98 نقدا. وتوجيه الاتهام بالاحتيال وتحويل أموال مسروقة إلى الولايات المتحدة، وقد أجاب لوزارينكو في الجلسة الافتتاحية بتاريخ 13 حزيران 2000 بأنه غير مذنب. وقد نشأت هذه القضية جراء أنشطة تحقيق امتدت إلى عامين كاملين تعاونت فيها الشرطة الفدرالية الأمريكية وأجهزة التحقيق في سويسرا إضافة إلى جهات أمنية في روسيا الاتحادية وأكرانيا، وجرى التحقيق في مصادر هذه الأموال التي تبين أنها نجمت عن استغلال رئيس الوزراء لمهام وظيفته هذه التي تولاها في الفترة ما بين أيار 96 وحتى تموز 97، وجراء تلقيه مبالغ نقدية من أفراد ومؤسسات ورشاوى لتسهيل تنفيذهم لأعمالهم، وتعد هذه القضية أول قضية وفق قانون غسيل الأموال الامريكي تستخدم الاجراءات فيها بشأن أنشطة ارتكبت خارج الولايات المتحدة وتتعلق بشخص من خارجها، وتستند المحكمة في اختصاصها إلى أن جزءً من الأنشطة الجرمية في بعض الحالات قد ارتكب داخل الولايات المتحدة، وجزءً آخر من الأنشطة كانت الولايات المتحدة فيه محطة لعمليات التحويل وادماج المبالغ محل الجريمة ضمن النظام المالي الأمريكي وإعادة تحويلها إلى جهات أجنبية أخرى، إلى جانب ايداع النقود في بنوك الولايات المتحدة وشراء موجودات ومشروعات فيها": عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، 2006، ص31.

ومن المزايا التي يعطيها الإنترنت لعملية غسيل الأموال السرعة واغفال التوقيع وانعدام الحواجز الحدودية بين الدول وتسهيل تحويل الأموال بواسطة الإنترنت وضمان تشفير وتأمين العملية وعدم ترك أي اثار (السند، 2005، ص76).

الفرع الثاني: التجسس الإلكتروني

وقد تكون المعلومات التي يتم التجسس عليها معلومات شخصية وقد تكون اجتماعية وقد تكـــون ذات قيمة اقتصادية أو سياسية أو حربية أو عسكرية أو تتعلق ببطاقات ائتمان. ويتم التقاط هذه البيانـــات والمعلومات بصور غير مشروعة (تجسس) باستخدام أسلوب ترجمة كلمات المرور من خـــلال التعقــب والتسلل للبرامج التي تتجه إليها أكثر أسماء المستخدمين وسرقة كلمات المرور التي تدون في قوائم ملفات كلمات المرور ثم تتم عملية مقارنة للبرامج المتعقبة لكلمات المرور المشفرة مع قاموس للكلمات العامـــة بحيث إذا ما تقاربت كلمات المرور المتلقطة مع الكلمات الموجودة في القاموس فإن المجرم المعلومـــاتي يحصل على اسم مستخدم جديد وكلمة مرور جديدة يستخدمها للولوج إلى النظام وإجراء التلاعــب فـــي البيانات وإجراء بعض العمليات كالتحويلات البنكية من الحسابات. ويمكن أن يتم التجسس الإلكتروني من خلال سرقة نصوص ملفات تحتوي على معلومات أو بيانات ذات اعتبار، كما قد يتم التجسس من خـــلال الأجهزة الحكومية التي باتت تستخدم التقنيات المعلوماتية للحصول علـــى بعــض المعلومـــات المتعلقـــة بالخصوم مثل ذلك التجسس التقليدي (الشوابكة، محمد، 2004، ص167-168).

وقد ساعدت تقنيات المعلومات والتطور التكنولوجي بتحول وسائل التجسس من الطرق التقليديـــة إلى الطرق الإلكترونية خاصة مع استخدام الإنترنت وخاصة في ظل ضعف الوسائل الأمنية المستخدمة لحماية الشبكات من التجسس. ولا يقتصر الخطر في التجسس على العابثين من مخترقي الأنظمة أو مـــا يعرفون اصطلاحاً (hackers) لأن مخاطر هؤلاء تعد محدودة وتقتصر عادة على العبــث أو اتـــلاف المحتويات، وهذا يمكن التغلب عليه باستعادة نسخة أخرى مخزنة، إنما يكمن الخطر الحقيقي في عمليات

التجسس التى تقوم بها الأجهزة الاستخباراتية للحصول على اسرار ومعلومات الدولة، وافـشائها لـدول أخرى أو استغلالها بما يضر بالمصلحة الوطنية لتلك الدولة.

مثال على ذلك أنه تم الكشف عن وجود شبكة دولية ضخمة للتجسس الالتكروني تعرف باسم (ECHELON) وتعمل تحت اشراف وكالة الأمن القومي الامريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كل من كندا وبريطانيا واستراليا ونيوزيلندا، لرصد المكالمات الهاتفية والرسائل بكافة أنواعها المرسلة برقياً أو تلكسياً أو فاكسياً أو إلكترونياً، وتتعامل هذه الشبكة مع الأهداف غير العسكرية وتعترض كميات هائلة جداً من الاتصالات والرسائل الالكتروينة .

ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل يتعداه إلى المعلومات التجارية والاقتصادية والثقافية (داود، 2000، ص 62). ويتم الاستعانة في عمليات التجسس بالاقمار الصناعية التي تصمم لالتقاط الاتصالات التي تجرى عبر الأجهزة اللاسلكية والهواتف المحمولة والإنترنت، ثم تحول هذه الاتصالات من خلال أجهزة كمبيوتر متطورة لتحليلها، وذلك كما في الولايات المتحدة.

ومن خلاله يمكن تنفيذ هجمات على الأهداف العسكرية، أي الأهداف العسكرية المرتبطة بشبكات المعلومات، وتعد هذه الهجمات نادرة الحدوث لأنها تحتاج معرفة عميقة بطبيعة الهدف، وطبيعة المعلومات المطلوبة وهذه المعرفة لا تمتلكها إلا الحكومات، كما أن الحكومات تقوم عادة بعزل المعلومات العسكرية الحساسة عن العالم، ولا تقوم بتوصيل أجهزتها مع العالم الخارجي، ويتم الوقاية من هذه الهجمات من خلال وضع نظم موثوقة للتحقق من شخصيات المستخدمين، والتحديد الدقيق لطبيعة المعلومات التي يسمح الوصول إليها.

الفصل الرابع

مكافحة الإرهاب الإلكتروني

مقابل وجود الخطر الإرهابي ووجود الجرائم الإرهابية في كثير من مناطق العالم لا بد من القول بأن هناك آليات وجهود حثيثة ومستمرة لمكافحة هذا الخطر وهذا ما اتضح في جميع مراحل التاريخ وعلى كافة المستويات الدولية والوطنية وفي كافة المجالات والإجراءات والتدابير اللازمة. وبالنسبة لجميع صور الإرهاب.

ومن هذا المنطلق أيضاً لا بد من التقرير بأن مكافحة الإرهاب بحد ذاتها تواجه كثير من الصعوبات، وهذا الأمر بالنسبة للإرهاب التقليدي، فكيف يكون الأمر عندما يتعلق الأمر بالفضاء الإلكتروني، حيث الانتشار الواسع على الشبكة وسهولة التخفي وسهولة ارتكاب الجرائم وتدمير آثارها وما إلى ذلك من خصائص تدور حول الجرائم الإلكترونية.

بالتالي فإن مزيد من الجهود يجب أن تبذل في هذا المجال مع عدم إغفال وإنكار دور الوسائل التقليدية في مكافحة الإرهاب، إذ أنه في إطار مكافحة الإرهاب الإلكتروني يمكن القول باستخدام الإجراءات والجهود التقليدية في مكافحته إلى جانب وسائل جديدة مبتكرة في إطار التكنولوجيا الإلكترونية.

وهذه المكافحة تتطلب اتخاذ مجموعة من المظاهر، منها ما هو على المستوى الوطني ومنها ما هو على المستوى الدولي، اذ لا تكفي الجهود التي تبذلها دولة بمفردها وبمعزل عن الدول الأخرى، لأن

مكافحة الإرهاب أمر يحتاج التكاتف، وعقد المعاهدات والمؤتمرات الدولية، والتصدي التشريعي، والتعاون الدولي، واتحاد الشركات والكيانات الاقتصادية الكبرى في مجال تعزيز أمنها الإلكتروني (الجنبيهي منير والجنبيهي ممدوح، 2005، ص179).

من هنا ترى الباحثة أن يتم تناول هذا الفصل من خلال المباحث الآتية:

المبحث الاول: الصعوبات والتدابير في مكافحة الإرهاب الإلكتروني

المبحث الثاني: الجهود الدولية في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

المبحث الثالث: الجهود الإقليمية والوطنية في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

المبحث الأول

الصعوبات والتدابير في مجال مكافحة الإرهاب الإلكتروني

من أهم ما تبين لنا من خلال فصول الدراسة المختلفة أن الإرهاب بصورتيه التقليدية والإلكترونية يواجه صعوبات متعددة في مجال مكافحته، وهذا ما يدفعنا إلى البحث في الجهود التي من الممكن أن تساعد في مكافحته والتقليل من آثاره وأخطاره، وفي هذا السياق يجب بداية التعرف على هذه الصعوبات التي تواجه مكافحة الإرهاب بصورتيه.

ومن جانب آخر تجدر الاشارة إلى أنه من الأولوية بمكان الحديث عن التدابير اللازمة لمكافحة الإرهاب بصورتيه التقليدية والإلكترونية. وهنا يمكن القول أن الصعوبات ذاتها تلقي بظلالها على هذه التدابير من حيث صورها وأنواعها، فكيفما تكون الصعوبات نكون أمام حاجة لنوع من التدابير ترتبط بهذه الصعوبات وصورها وأشكالها.

وتتنوع هذه التدابير ضمناً بتنوع الصعوبات، ومن هذه التدابير صورتين رئيسيتين هما تدابير تتعلق بالمجال التشريعي من حيث النصوص القانونية والمعاهدات الدولية، ومجموعة أخرى من التدابير منها ما هو اجرائي ومنها ما هو تقني وفني وغير ذلك، وتطلق عليها الباحثة التدابير العادية تمييزاً لها عن التدابير الفنية.

لذا فإن الباحثة تقسم هذا المبحث إلى المطالب الاتية:

المطلب الاول: الصعوبات التي تواجه مكافحة الإرهاب الإلكتروني

المطلب الثاني: التدابير العادية في مكافحة الإرهاب الإلكتروني

المطلب الثالث: التدابير الفنية في مكافحة الإرهاب الإلكتروني

المطلب الاول: الصعوبات التي تواجه مكافحة الإرهاب الإلكتروني

تشير الباحثة بداية إلى أن هناك مجموعة من العقبات التي تعيق التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وهي بحد ذاتها ذات الصعوبات والعوائق التي تعيق مكافحة الإرهاب الإلكتروني باعتباره صوره من صور الجرائم الإلكترونية كما تبين في الفصل الثاني من هذه الدراسة.

أولاً: هناك عدد من الصعوبات بشكل عام تواجه عملية مكافحة الجرائم المعلوماتية مثل: سهولة إخفاء الجريمة، فهذه الجريمة غالباً ما تكون مستترة وخفية ترتكب في اطار من السرية من قبل شخص وتعامله مع جهاز مربوط بالشبكة. ونقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في مجال التكنولوجيا والفضاء الإلكتروني. وصعوبة الوصول إلى مرتكبي أغلب الجرائم المعلوماتية لسهولة اختبائهم وعدم كشف هوياتهم (العادلي، 2009 16).

ثانياً: ومن الصعوبات التي تواجه التعاون الدولي في مجال التحقيق في الجريمة الإلكترونية ومكافحتها ما

يأتي (السند، 2005، ص41-42):

أ. عدم وجود اتفاق عام مشترك بين الدول حول الأفعال الجرمية أي التي تعد جرائم من عدمها. وعدم الوصول فيما بينها أيضاً إلى مفهوم عام موحد حول النشاط الذي يمكن الاتفاق على تجريمه، فهناك من الأفعال ما يعد مجرماً في بلد ما، وهو ليس كذلك في بلد أخرى، بالتالي فإن ذلك يشكل صعوبة في مجال تحديد الأفعال المجرمة تمهيداً لمكافحتها.

ب. اختلاف مفاهيم الجريمة باختلاف الحضارات أي من دولة أو مجموعة من الدول لأخرى وباختلاف ثقافاتها، اذ قد تختلف نظرة كل نظام قانوني أو اجتماعي أو ثقافي للجريمة من حيث أهميتها أو من حيث التقليل من شأنها، وهذا بطبيعة الحال يؤثر في مكافحة هذه الجرائم من حيث الاهتمام بموضوع المكافحة أو التقليل من شأن هذه الجرائم وآثارها.

ج. عدم وجود معاهدات دولية لمواجهة المتطلبات الخاصة بالجرائم الإلكترونية خاصة الجرائم الإرهابية الإلكترونية، رغم أنه قد تم التوقيع في تشرين الثاني من عام 2001 في بودابست على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت لتشكل الأداة القانونية الأولى الملزمة في إطار الإنترنت(التوقيع على الاتفاقية الدولية لمكافحة الإرهاب عبر الإنترنت، 2001/11/23، بدون رقم صفحة).

د. وجود عوائق ومشكلات قانونية وفنية فيما يتعلق بالقيام ببعض إجراءات التحقيق وتعقب وملاحقة مرتكبي هذا النوع من الجرائم، مثل القيام بإجراء التفتيش في ظل الأنظمة المعلوماتية خارج حدود الدولة وضبط المعلومات المخزنة فيها، أو الأمر بتسليمها، ومثل الانابة في مجال التحقيق بالنسبة لهذه الجرائم باعتبارها عابرة للحدود، وغير ذلك من إجراءات يتطلبها التحقيق في بيئة الحاسب

الالي والانترنت.

ثالثاً: صعوبة الإثبات في هذه الجرائم، ويرجع ذلك إلى عوامل هي (العادلي، 2009، ص16-17):

أ. الطبيعة الخاصة للدليل في الجرائم المعلوماتية، اذ أنه ليس دليلاً مرئياً يمكن فهمه بالقراءة، ويتمثل ببيانات غير مرئية لا تفصح عن شخصية معينة عادة .

ب. صعوبة الوصول إلى الدليل: فبإمكان المجرم المعلوماتي زيادة صعوبة عملية ضبط أي دليل يدينه من خلال استخدامه لكلمات مرور بعد تخريب الموقع مثلاً أو باستخدامه تقنيات التشفير.

ج. سهولة محو الدليل: من خلال مجرد الضغط على بعض الأحرف أو الكبسات على الكيبورد أو باستخدام الفأرة.

د. أدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة، كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات ، ولهذا فإنها تثير اشكاليات أمام القضاء ومشكلات عديدة، خاصة فيما يتعلق بقبولها وحجيتها والمعايير اللازمة لذلك.

رابعاً: إحجام الجهات والأشخاص المجني عليهم عن الإبلاغ عن الجرائم المعلوماتية، خاصة في الجهات المالية كالمصارف والبنوك ومؤسسات السمسرة، لأنها تفضل كتمان أمر هذه الجرائم تفادياً للآثار السلبية التي قد تنجم عن كشفها أو اتخاذ الإجراءات القضائية تجاهها لأن ذلك قد يؤدي إلى تضاؤل الثقة فيها من قبل المتعاملين معها (العادلي، 2009، ص17).

خامساً : صعوبات في ضبط وتوصيف جرائم المعلوماتية، بسبب الطبيعة الخاصة لهذه الجرائم حيث تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود (العادلي، 2009، ص17).

سادساَ: التعارض بين التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية، إذ أن التفتيش بحثاً عن هذه الجرائم وأدلتها يتم غالباً في نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وهذا يؤكد أن الأمر قد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة به، بسبب التشابك بين الحواسيب المختلفة، وانتشار الشبكات الداخلية على مستوى المنشآت، وانتشار الشبكات المحلية والإقليمية والدولية على مستوى الدول، وهذا الامتداد في التفتيش قد يمس حقوق الخصوصية المعلوماتية لأصحاب تلك النظم التي يتم الامتداد إليها (العادلي، 2009، ص17).

سابعاً: فكرة الاختصاص والطبيعة الدولية للجرائم المعلوماتية، فعادة ما يكون مرتكبي الجرائم المعلوماتية أشخاص من خارج الحدود، وتمر الجريمة المعلوماتية عبر شبكات معلومات وأنظمة معلومات خارج الحدود، الأمر الذي يثير اشكاليات وتساؤلات حول الإختصاص القضائي لنظر هذه الجرائم، كما أن امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود تحتاج إلى تعاون دولي شامل في مجال مكافحتها وذلك دون التعرض للسيادة الوطنية للدول المعنية (العادلي، 2009 17).

المطلب الثاني: التدابير العادية في مكافحة الإرهاب الإلكتروني

ترى الباحثة أنه ومن الناحية الاجتماعية والأمنية فإن الوقاية من الاعتداءات وجرائم الكمبيوتر تعتمد على ممارسة أساليب الوقاية التي تتبعها المؤسسات الأمنية، ويتمثل الدور الاجتماعي والأمني في تعاون ضحايا الجرائم مع رجال الأمن المكلفون باستقصاء جرائم الحاسب الالي.

ويلاحظ من خلال البحث أن تدابير أو أساليب مكافحة الإرهاب بصورتيه تتفقان نوعاً ما، وتقسم إلى نوعين وسائل منع، ووسائل قمع:

- وسائل المنع: أي وضع الخطوات والإجراءات اللازمة لمنع الإرهاب قبل وقوعه فإذا ضبط الشخص الإرهابي قبل العملية حتى لو توافرت أدوات الجريمة فإنها لن تقع، كذلك الحال إذا تم ضبط أدوات الجريمة فإنها لن تقع، كذلك الحال إذا ما عرفنا الهدف أو محل الجريمة المستهدف وتم تأمينه تأميناً صحيحاً وكافياً فلن تتم الجريمة، بالتالي يمكن القول أن الإرهاب ثلاثي الأبعاد بشموله المحاور السابقة(بوادي، 2004، ص47). وهذه الأبعاد هي: الإرهابي، والأدوات الإرهابية، والهدف المستهدف من الإرهاب.
- المكافحة بالقمع (بعد ارتكاب الجريمة): أي اتخاذ التدابير والإجراءات اللازمة لضبط مرتكبيها في أسرع وقت ممكن وبفعالية شديدة وبأقل قدر من الخسائر لما لذلك من أثر شديد في إعادة الثقة لنفوس المواطنين وعامة الناس وردع الإرهابيين، وحملهم على عدم العودة لارتكاب الجرائم.

ويجب أن تتم إجراءات الردع أيضاً بنوع من الشدة لعدم تشجيعهم على مزيد من العنف والعنف المنظم الذي يعمل على انهيار هيبة الدولة وسيادة الفوضى والإرهاب(بوادي،2004، ص54).

ويمكن تفصيل هذا الأساليب كالآتي:

أولاً: المشاركة الشعبية من خلال التوعية والتثقيف الفكري ومحاولة القضاء على أسباب الإرهاب والتطرف (بوادي، 2004، ص56):

ففي مجال مكافحة الإرهاب التقليدي والتي يمكن الأخذ بها في الإرهاب الإلكتروني متى تم التعرف على أسباب الإرهاب، فإذا كان للفراغ الفكري دور فيه فإن من أنسب الطرق القضاء على هذا الفراغ من خلال وسائل كالآتي (نظمي، 2010، ص12-13):

- تثقيف الوالدين لأبنائهم وتوعيتهم منذ الصغر.
- أن يحرص الإنسان على القراءة والتثقيف بمختلف الجوانب والعلوم.
- متابعة الحوارات والنقاشات الثقافية والفكرية والعلمية والمشاركة منها.
- عدم انشغال الذهن بأمور من شأنها تشويش الفكر.
- الالتزام بالمبادئ والمناهج الفكرية لتحقيق الاستقرار الفكري.

ثانياً: تنشيط المواقع الصالحة التي تدعو إلى التعايش السلمي بين الحضارات المختلفة ونشر راية السلام والمحبة والتسامح والإنسانية بين المجتمعات (مجلة بريس المغرب الإلكترونية، الارهاب الالكتروني، بدون رقم صفحة).

ثالثاً: التوعية الأمنية لتحقيق الأمن الفكري، وغرس المفاهيم الأمنية في العقول الناشئة، ومن المسائل الهامة في تحقيق الأمن الفكري وتكريسه دور الأسرة والمجتمع، والتربية على المثل والقيم والمبادئ والأخلاق الحميدة، والتركيز على حماية الأفراد من الانحرافات الفكرية التي تولد الكثير من المشكلات الاجتماعية، والتنشئة الدينية السليمة بعيداً عن التطرف والغلو، والتركيز على قيم المجتمع وقوانينه (نظمي، 2010، ص21). ومما يساهم في مكافة هذه الجرائم نشر التوعية حول أضرار هذه الأعمال والنتائج المترتبة على استخدامها وتجريم مستخدميها (المصري، 2011، بدون رقم صفحة). وتشمل هذه الوسائل إلى جانب التوعية الأمنية التدريب في مختلف الجوانب السلوكية والاقتصادية والاجتماعية والسياسية والإدارية والقيادية. وتحقيق الوسائل البشرية والفنية والمادية اللازمة (بوادي، 2004، ص56).

رابعاً: تعزيز التعاون والتنسيق بين الدول والحكومات والمؤسسات الدولية المعنية، وتوحيد الجهود المختلفة لفرض الرقابة الكافية على ما يقدم من خلال الشبكة، وتقوية وتعزيز حماية المواقع الهامة، وسد ثغراتها، وتوفير التقنيات اللازمة لمواجهتها، ولفت نظر المجتمع الدولي لإبرام إتفاقيات تعاون تكافح هذه الجرائم (مجلة بريس المغرب، الإرهاب الإلكتروني، بدون رقم صفحة). ويشمل التعاون أيضاً ذلك التعاون بين مزودي خدمة الإنترنت من خلال قيامهم بالإبلاغ عن الأنشطة الإرهابية التي تتضمن أفعالاً

مخلة بالأمن والنظام، أو تتضمن أفعالاً اجرامية كالتهديد بالموت أو الإصابة الجسدية الخطيرة لأي شخص.

خامساً: تدابير مالية من خلال حث الدول على تجميد أموال الإرهابيين ومن يرتبط بهم من أشخاص وكيانات سواء كانوا أشخاص طبيعيين أو اعتباريين(خريسات، 2006/2005، ص54).

سادساً: التدابير التشريعية

ويعني ذلك التدخل التشريعي من خلال تجريـــــــم ما تقوم به المنظمات الإرهابية بجميع أعمالها التخريبية والتجسسية والحربية وتشديد العقوبات على هذه الأفعال. فلمواجهة الإرهاب تشريعياً يكون من الضرورة بمكان مواكبة التطور الحاصل في مجال الجرائم المعلوماتية من خلال المواجهة التشريعية الكافية، والتصدي اللازم للتعامل مع هذه الجرائم من خلال ايجاد قواعد قانونية غير تقليدية كافية لمعالجة الإجرام المعلوماتي غير التقليدي، وكافية للتعامل معها (العادلي، 2009، ص3. وخريسات، 2006/2005، ص55. والبند الثاني من قرار مجلس الامن رقم 1373، 2001).

المطلب الثالث: التدابير الفنية الإلكترونية في مكافحة الإرهاب الإلكتروني

يتم ذلك من خلال مجموعة من الوسائل الاجرائية التي يقصد بها تقوية أجهزة التحريات والمعلومات (وقد تكون ضعيفة سابقة) من قبل الأجهزة المعنية والتي تؤدي إلى ضبط مرتكبي الجرائم

والمساهمة في ردعهم عن ارتكاب هذه الجرائم والمساهمة في الإجهاض المبكر للعمليات الإرهابية وكشف المخططات الإجرامية للإرهابيين والهجوم عليهم وضربهم بالضربة الاستباقية. وذلك بعد جمع المعلومات اللازمة والدقيقة عنهم وعن مخططاتهم (بوادي، 2004، ص55).

تتخذ التدابير الفنية الجانب الأهم في مجال مكافحة الإرهاب خاصة التكنولوجي أو الإلكتروني، وذلك مع عدم التقليل من شأن التدابير غير الفنية، إلا أنه في مجال مكافحة الجرائم المعلوماتية والإرهاب الإلكتروني الذي يتم أساساً بوسائل فنية وإلكترونية، فإن قيمة هذه التدابير تظهر بشكل أكثر جلاءً.

بالتالي فإن اللجوء إلى هذه التدابير من قبل الأجهزة الأمنية يساعد أجهزة الحاسب الآلي على مقاومة الاعتداءات الموجهة اليها أو تعطيلها. ومن هذه الوسائل على سبيل المثال وضع واعتماد سياسيات قوية لدى الشركات المعنية، وضرورة تنفيذها من قبل العاملين فيها، كاستخدام جدران الحماية، وعدم تنزيل ملفات الارتباط من أشخاص مجهولة، واستخدام برامج حماية قوية.

وترى الباحثة بالاتفاق مع كثير من الآراء أن مقاومة الجرائم والاعتداءات الإلكترونية تتم من خلال:

أولاً: مقاومة فنية بحتة، مثل (نظمي، 2010، ص21):

أ. تشفير البيانات المهمة المنقولة عبر الانترنت.

ب. ايجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.

ج. توفير برامج الكشف عن الفيروسات والمقاومة لحماية الحاسب.

د. عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية مع عمل وسائل التحكم في الدخول إلى المعلومات والمحافظة عليها.

ه. توزيع مهام العمل بين العاملين.

ثانياً: المقاومة الفنية النظامية

من خلال توظيف التكنولوجيا بأسلوب علمي لتعقب الإرهابيين ومكافحة الجريمة وخدمة رجال الأمن، عن طريق فحص وكشف البصمات، وتتبع البيانات، واسترجاعها بسرعة فائقة ودقة عالية، وتبادل المعلومات التي تساهم في الكشف عن مرتكبي الأعمال الإرهابية وتعقبهم(نظمي، 2010، ص21).

ومن صورها:

أ. مراقبة الإنكشافات: أي تحديد الثغرات الأمنية في نظم المعلومات مثل البناء الفيزيقي والأقفال وجدران الحماية والمباني والسلامة العامة وأجهزة الحاسب وكلمات الدخول(البداينة، 2002، ص305).

ب. إيجاد الثغرات في الحاسب والشبكات: وتبدأ هذه العملية من خلال تثبيت البرنامج أي برنامج نظام التشغيل، حيث يتم وضع برامج أخرى عليه لإيجاد أي هجمات أو أخطار عليه(البداينة، 2002، ص305).

ج. من وسائل المكافحة انشاء ادارات متخصصة في وزارة الداخلية والجهات الأمنية لمتابعة ومراقبة الأنشطة الإلكترونية والوقاية من الجريمة المعلوماتية(الجنبيهي منير والجنبيهي ممدوح، 2005، ص230).

د. مراقبة المنشورات الأمنية: أي مواكبة النشر العلمي في المجال الأمني ومن المنظمات المهتمة بذلك مركز التنسيق لفريق الاستجابة لطوارئ الحاسب (CERT) و (SANS) وهناك مواقع كثيرة على الإنترنت تزود الراغبين بكل جديد في مجال الثغرات والفيروسات(البداينة، 2002، ص323).

وفي هذا الصدد أفادت مجلة "دير شبيغل" الألمانية أن الجيش الألماني بصدد إنشاء كتيبة عسكرية متخصصة في مكافحة الإرهاب الإلكتروني أو النزاعات الإلكترونية، ويطلق عليها اسم (قسم العمليات المعلوماتية والشبكات الإلكترونية)، وأنها ستتألف من 76 جندياً متخصصاً في هذا المجال، وأنها ستعمل بسرية تامة، لحماية المؤسسات والمصالح الالمانية من الاعتداءات الإلكترونية، وأنه سيتم تدريبهم على تطوير اساليب جديدة لاختراق الشبكات الإلكترونية والتجسس والتشويش عليها وهدمها (خبر بعنوان، كتيبة عسكرية لمكافحة الإرهاب الإلكتروني، موقع عيون العرب، http://vb.arabseyes.com/t94470.html، بدون رقم صفحة).

ثالثاً: ترشيح الدخول على الإنترنت

لقد تغلغل الانترنت وغزا العالم بأسره، حتى بات الجميع غير قادرين على العيش بعزله عن التواصل مع مجريات الأحداث في العالم من خلال شبكة الانترنت. إلا أن من الحلول الممكنة للسيطرة أو التقليل من مخاطر الدخول للانترنت هو عملية ترشيح الدخول. ويتم ذلك من خلال حجب المواقع الضارة، التي

تستخدمها الجماعات والتنظيمات الإرهابية، والتي تدعو إلى الفساد والشر، كتلك التي تدعو إلى الإرهاب وتحرض عليه وتساهم في تعلمه وتحض على العدوان (السند، 2005، ص25). وتلجأ الدول عادة إلى استخدام هذه التقنيات من خلال حجب بعض المواقع الضارة على الشبكة وهذا قد يستدعي تركيب أجهزة وأدوات تعمل على فلترة وتنقية المواقع وحجب بعضها.

رابعاً: التشريعات اللازمة لضبط التعاملات الإلكترونية

بسبب المخاطر التي تحيط بشتى أنواع التعاملات الإلكترونية باتت الحاجة ملحة لايجاد تقنية للمعلومات تسمح بضبط التعاملات الإلكترونية، الا أنه ومع التطورات الحاصلة في المجال التكنولوجي لا زال هناك بطء من قبل الجهات المعنية بذلك. ومن هنا ظهرت الحاجة لإعداد الأنظمة اللازمة لتحقيق الاستفادة القصوى من تقنية المعلومات، ومراجعتها، وحماية المتعاملين من مخاطرها. ويمكن أن تتم أنظمة الضبط هذه من خلال توفير الأنظمة واللوائح اللازمة لتنظيم سلوك الأفراد والمؤسسات في مجال التعامل مع تقنية المعلومات، دون أن تكون هذه الأنظمة واللوائح قيداً على حرية المجتمع (السند، 2005، ص26-27).

ومن الأمثلة في هذا الصدد وضع أنظمة لضبط التعاملات الإلكترونية وأنظمة لتجريم الاعتداءات التي تتم ممن خلال الانترنت، وأنظمة لتجريم العدوان الإلكتروني، وأنظمة لحماية التبادلات والتجارة الإلكترونية، وأنظمة للحد من الاختراقات الإلكترونية (الجنبيهي منير والجنبيهي ممدوح، 2005، ص239-240. والسند، 2005، ص28-29).

خامساً: أنظمة الحماية الفنية من الاعتداءات الإلكترونية

تتمثل هذه الأنظمة بصياغة تقنيات إلكترونية تكفل حماية التعاملات الإلكترونية من ناحية فنية وذلك بعد تنامي مخاطر التكنولوجيا الحديثة. حيث تعمل هذه الأنظمة لمقاومة الجرائم والاعتداءات الإلكترونية. وتتم المقاومة الفنية من خلال الوسائل الآتية (السند، 2005، ص30. الجنبيهي منير والجنبيهي ممدوح، 2005، ص234-235):

أ. تشفير البيانات المهمة المنقولة عبر الإنترنت

ب. إيجاد نظام أمني متكامل، يقوم بحماية البيانات والمعلومات

ج. توفير برامج الكشف عن الفيروسات ومقاومتها، لحماية الحاسب الآلي، والبيانات، والمعلومات.

د. عدم تداول المعلومات الأمنية والهامة من خلال شبكات الحاسب الآلي المفتوحة، وايجاد وسائل للتحكم بالدخول إلى المعلومات والمحافظة على سريتها.

ه. توزيع المهام والوظائف التقنية بين العاملين، فيتم اعطاء كل شخص وظيفة من الوظائف بحيث لا يجمع بين وظيفتين معاً، فمثلاً لا يتم إعطاء المبرمج وظيفة تشغيل الحاسب الآلي إضافة إلى وظيفة البرمجة. كما يمكن أن يتم توزيع مهام البرنامج الواحد على مجموعة من المبرمجين الأمر الذي يجعل كتابة برامج ضارة أمراً صعباً.

و. بناء النظم الآمنة: يتم ذلك بشراء الأجهزة والبرمجيات التي تحقق أكبر قدر من الأمن للمعلومات السرية وقد قامت وزارة الدفاع الأمريكية بعدة دراسات ولقاءات ومشاريع لبناء معايير موثوقة لتقييم النظم(البداينة، 2002، ص326).

سادساً: تحقيق الأمن المعلوماتي للكيانات الاقتصادية

كالشركات والبنوك وما شابهها من ركائز اقتصادية اذ أن تحقيق الأمن الإلكتروني لهذه الكيانات يعد من الأولويات التي يجب أن تأخذ بالاعتبار لأن اختراق هذه المنشآت وما قد ينجم عنه من خسائر مادية ومعنوية هائلة لتلك المنشآت ومستوى سمعتها من الثقة والأمان (الجنبيهي منير والجنبيهي ممدوح، 2005، ص233).

سابعاً: الحفاظ على المعلومات على الشبكة

تعد المعلومات ذات أهمية بالغة بالنسبة لجميع الفئات والشرائح والمستويات، وتحرص عليه الهيئات والمنظمات والدول والأفراد. والمعلومات شيء لا يمكن تعويضه، بخلاف البرامج والادوات التي يمكن تعويضها. ولأن المعلومات أهم ما يمكن أن تسعى هذه الشرائح للمحافظة عليه فيجب اتباع مجموعة من الإجراءات اللازمة لحمايتها من الاعتداء، منها (السند، 2005، ص34-35):

أ. تمزيق المخرجات غير المرغوب بها بواسطة آلات خاصة قبل إلقائها، بالتالي يجب عدم إلقاء مخرجات الحاسب الآلي، أو شريط تحبير الطابعة، لأنها قد تحتوي على معلومات هامة قد تصل إلى أشخاص غير مصرح لهم الاطلاع عليها.

ب. استخدام كلمات السر للدخول إلى الحاسب الآلي، وتغيير هذه الكلمات من فترة لأخرى، وعدم استخدام الكلمة الواحدة أكثر من مرة ولفترة أطول.

ج. منع ومحاولة منع محاولات الدخول غير النظامية، من خلال عمل طرق تحكم داخل النظام، كانشاء

ملفات لتسجيل جميع الأشخاص الذين وصلوا أو حاولوا الوصول إلى أي جزء من البيانات ومعلوماتهم.

د. توظيف أشخاص تنحصر مهمتهم فقط في متابعة مخرجات برامج الحاسب الآلي باستمرار للتأكد من أنها تعمل بشكل صحيح.

ه. تشفير البيانـــــــات خاصة المهمة منها والمنقولـــــــة عبر وسائل الاتصالات، كالأقمار الصناعية والألياف البصرية، ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل.

و. عمل نسخ احتياطية من البيانات المخزنة.

ز. استخدام وسائل تقنية حديثة ومتطورة، تضمن دخول الأشخاص المصرح لهم فقط، إلى أقسام مركز الحاسب الآلي وذلك من خلال وسائل وتقنيات حديثة كالأجهزة التي تعمل على بصمة العين، أو اليد، أو الصوت.

ثامناً: جدران الحماية

تقوم هذه التطبيقات بتأمين المنافذ ports التي تحصل من خلالها مختلف التطبيقات على خدمات الإنترنت، وهذه المنافذ تحدد برمجياً ضمن نظم التشغيل أو التطبيقات المستخدمة، وفي كثير من الأحيان لا يستعمل المستخدم كافة هذه المنافذ مما يجعله يسهو عن تأمينها وحمايتها، مما يشكل فرصة مثالية للهكرة للنفاذ إلى النظام. وتعمل برمجيات الجدران النارية كمصفاة ومفلتر تمنع وصول الطلبات المشبوهة إلى الأجهزة التي توجد بها، وذلك بالاعتماد على السياسات التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات التي يسمح للعاملين بالمؤسسات النفاذ إليها. وهي أداة تعمل على تصفية أو حجز مرور

البيانات بين الشبكة الداخلية المحمية، والشبكة الخارجية التي نخشى منها، والهدف منه حجز كل ما هو غير مرغوب فيه خارج البيئة المحمية. وتكون هذه الجدران على ثلاثة أنواع هي: الموجه الحاجب: Screening Router، والوسيط Proxy، والحارس Guard (داود، 2000، ص159).

تاسعاً: تأمين حسابات المستخدمين ونظم التحقق من الهوية

وتتمثل بتقنيات التحقق من الهوية وخصوصاً أساليب التحقق البيولوجي من الهوية التي تتم بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص، ومن وسائل التأمين أيضاً كلمات السر وأسماء المستخدمين، وهناك وسائل تعتمد على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم. أما نظم التحقق من الهوية فتتكون من ثلاث تقنيات هامة هي: خدمات الأدلة Directory Services، وهيكلية المفاتيح العامة Public Key Infrastructure، والشبكات الافتراضية الخاصة Virtual Private Networks ، ونبحثها كالآتي (داود، 2000، ص104-109):

أ- خدمات الأدلة: وهي عبارة عن قواعد بيانات خاصة، ذات مستوى عال من الأمان، ومصممة لجمع وإدارة المعلومات المتعلقة بمستخدمي الشبكات، تقوم على جمع كلمات السر وأسماء المستخدمين، وسماتهم البيولوجية، ويتم استخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بجميع مكوناتها، كالتطبيقات والأجهزة الخادمة والمجلدات، وشكل الشاشة التي يستعملها المستخدمين، وتدار بشكل مركزي من مكتب مدير الشبكة، دون حاجة لزيارة الأجهزة أو المستخدمين، ومن الشركات الرائدة في هذا المجال شركة نوفيل Novell.

ب- تقنية المفتاح العام: التي تقوم على تقنيات تشفير البيانات، أو بعثرتها بالاعتماد على علاقات رياضية خاصة تجمع بين مفتاحين أو كلمتين سريتين، أحدهما عام والآخر خاص. فعند إرسال كلمة رسالة فإن ذلك يعني أي نوع من المعلومات المتناقلة بين النظم الإلكترونية، بما في ذلك الأوامر التي تتناقلها التطبيقات بين بعضها البعض، فيقوم التطبيق الموجود على الجهاز بتشفيرها، أو بعثرة بياناتها، باستخدام كلمة سر غير معروفة لأحد غير المستخدم، ثم تشفيرها ثانية بالمفتاح العام للمستقبل، وتكون الوسيلة الوحيدة التي يمكن للمستقبل أن يتعامل بها مع الرسالة هي فك تشفيرها، أو إعادة ترتيب بياناتها، باستخدام مفتاحه الخاص أو كلمة السر أولاً، ثم استخدام المفتاح العام لفك الشيفرة الخاصة به. ويتم إصدار شهادات رقمية للمصادقة على صحة هذه المفاتيح من قبل هيئات عالمية وشركات خاصة كشركة RSA أو Verisign (فيري ساين).

ج- الشبكات الافتراضية الخاصة: وتعد أكثر الطرق أمناً للتحكم بالأشخاص الذين يمكنهم الولوج إلى الشبكة، وتتم هذه التقنية من خلال إقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ من خلالها إلا من يقوم بتحديده مدير الشبكة، فيقوم فقط المستخدمين المعينين من النفاذ عبر الشبكة، وإسقاط الحزم الواردة من أية جهة غيرهم، وتعتمد هذه التقنيات على بروتوكولات اتصالات آمنة وخاصة، أهمها بروتوكول IPSec .

د- أمن البرمجيات: وتأتي إلى جانب أية سياسة أمنية شاملة، وتعد من المسائل الصعبة لأنها تتطلب إجبار وتثقيف المستخدمين، ليقوموا بتحديث برمجياتهم واعتماد كافة الاصلاحات التي تعتمدها الشركات المنتجة بشكل مستمر، كي يضمنوا شمولية السياسات الأمنية المعتمدة لديهم، وهذا ما تصعب متابعته. وتهتم بعض الدول بما قد يظهر من اخطاء وثغرات، وتقوم بنشرها، مثل المجلة

التابعة للحكومة الأمريكية التي تصدر كل أسبوعين وينشر من خلالها قائمة بجميع العثرات والثغرات المكتشفة في البرمجيات وطرق تصليحها وهي موجودة على العنوان (http://www.nipc.gov/cybernotes/cybernotes.htm).

عاشراً: بعض الإجراءات الأخرى (البداينة، 2002، ص327 وما بعدها):

أ- الوعي الأمين والتدريب: من خلال إعلام الموظفين لسياسة أمن المعلومات في المنظمة التي يعملون بها وإحاطتهم بخطورة الحرب المعلوماتية وتدريبهم في مجال استخدام الممارسات الأمنية والتقنيات.

ب- تجنب الانهيار الكلي: وذلك من خلال التوزيع السليم للمعلومات وعدم وضعها في مكان واحد من خلال عمل نسخ احتياطية ووضعها في أماكن آمنة.

ج- إدارة الخطورة: والتي تمر بمراحل ثلاث هي تحليل الخطر وتحديد التهديدات وتقدير الخطورة.

د- الدفاع عن المجتمع المعلوماتي: وهذا واجب ملقى على عاتق الحكومات لتدافع عن الأمن المعلوماتي كما هو الحال بالنسبة لأنماط وصور الأمن الأخرى.

ه- سياسة التشفير.

و- حراسة المعلومات ورقابتها وذلك من خلال: التحكم بالدخول للأصول المعلوماتية. وسياسات السماح بالدخول، والرقابة عليه والتحكم به، وترشيح المعلومات (برامج ترشيح)، وجدران

الحماية الأمينة، ومرشحات البريد غير المرغوب به، ومرشحات البرامج غير المرغوب بهـــا، واكتشاف التطفل وسوء الاستخدام والرقابة في مكان العمل، وتفصيل الكشف التلقائي.

المبحث الثاني: الجهود الدولية في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

لقد تداخل العالم بفضل التكنولوجيا ببعضه البعض وغدا كالقرية الصغيرة، بسبب وسائل الاتصال والتقنيات المتطورة، والعلاقات المتنوعة التي تسود العالم، وقيام المصالح المتبادلة بين الشعوب، الأمر الذي اقتضى ظهور التعاون الدولي في كافة مجالات الحياة.

ومن الصور التي تطلبت التعاون بين الدول التعاون في المجالات الأمنية بين دول العالم عامة والدول العربية خاصة، ومنها ما هو في مجال الإرهاب، لأن التعاون والتكامل الأمني بين الدول أصبح أمراً حتمياً لأنه السبيل الوحيد إلى تغليب العقبات والمعوقات التي تواجه الدول عند محاولتها التصدي له (عبد الحميد، 1999، ص112).

وقد تنبهت الدول العربية للاخطار المحدقة بها، فعقدت كثير من المعاهدات والاتفاقيات لمكافحة الإرهاب، ودعم التعاون العربي في هذا المجال، ومن أهم هذه الاتفاقيات الاتفاقية العربية لمكافحة الإرهاب، التي تشكل أهم ركائز العمل العربي المشترك. وقبل ذلك نتحدث عن الجهود الدولية في مجال مكافحة الإرهاب.

وتلعب الدول الكبرى دوراً هاماً في هذا المجال، وفي هذا السياق نشير إلى اتهام الأمين العام السابق للامم المتحدة (فالدهايم) الدول الكبرى أنها تتحمل القسط الأكبر من مسؤولية تفشي ظاهرة الإرهاب وذلك للأسباب التالية (التل، 1998، ص18):

1. ممارسة حق النقض الفيتو في مجلس الأمن وتهاون الدول الكبرى في القيام بواجباتها الأمر الذي تسبب بعجز المنظمة عن القيام بواجباتها على أفضل وجه وبما يتفق مع حقوق الانسان.

2. تواطؤ الدول الكبرى أفشل المنظمة في تحقيق أهدافها في تحقيق التعاون الدولي وحل المشكلات الاقتصادية والاجتماعية بين الدول

3. الاعتداء على حقوق الشعوب المستضعفة واغتصاب حقوقها

والجهود الدولية تصب في مكافحة الجرائم والإرهاب وينطبق الوصف فيها على صورتي الإرهاب التقليدي والإرهاب الإلكتروني، وتتناول الباحثة في هذا المبحث هذه الجهود الدولية التي إما أن تكون على مستوى الهيئات الدولية ممثلة بالأمم المتحدة، واما جهود على مستوى الدول فيما بينها كالاتفاقيات الدولية وبعض المظاهر الأخرى للتعاون، ومن هنا فإن الباحثة تقسم هذا المبحث إلى مطلبين كالآتي:

المطلب الاول: جهود الأمم المتحدة في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

المطلب الثاني: جهود الدول في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

المطلب الاول: جهود الأمم المتحدة في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

يمكن للباحثة استعراض دور الأمم المتحدة في مكافحة الإرهاب وتنظيم العدالة الجنائية الدولية من خلال تناول دور الجمعية العامة للأمم المتحدة بداية ومن ثم دور مجلس الأمن الدولي، وذلك من خلال فرعين كالآتي:

الفرع الاول: دور الجمعية العامة للأمم المتحدة

ويمكن معالجته كالآتي:

أولاً: شددت الأمم المتحدة منذ التسعينيات على أهمية المباشرة بالعمليات والإجراءات التطبيقية في مجالات مكافحة الجريمة والعدالة الجنائية الدولية وشجعت على قيام لجنة جديدة للتنسيق بين الحكومات في هذا المجال ولعقد المؤتمرات العلمية والمتخصصة في هذا المجال. وأنشأت بعض المعاهد منها (شلالا، 2003، ص61-62):

أ. معهد الأمم المتحدة لمكافحة الجريمة ومعالجة الأحداث في آسيا والشرق الأقصى ومركزها اليابان، عام 1961).

ب. معهد مناطق أبحاث الأمم المتحدة حول الجريمة والعدالة في روما عام 1968.

ج. المعهد اللاتيني – أمريكي للأمم المتحدة لمكافحة الجريمة ومعالجة الأحداث في البرازيل عام 1975.

د. معهد هلنسكي لمكافحة الجريمة في فنلندا عام 1981.

ه. المعهد الأفريقي للأمم المتحدة لمكافحة الجريمة ومعالجة الأحداث في أوغندا عام 1989.

ثانياً: في المجال الإلكتروني أنشأت الأمم المتحدة بنك المعلومات والبريد الإلكتروني تحت اسم الشبكة الدولية الإعلامية للعدالة الجنائية (UNCIDIN) بهدف نقل الدراسات والأبحاث الصادرة عن المعاهد الجنائية إلى المنظمات الحكومية وغير الحكومية والعاملين في مجالات العدالة الجنائية والمهتمين والخبراء وغيرهم(شلالا، 2003، ص63).

ثالثاً: قرارات الجمعية العامة ذات الشأن

بالرجوع إلى قائمة قرارات الجمعية العامة للأمم المتحدة نجد أن هناك الكثير من القرارات التي تتعلق بالإرهاب ومكافحته وهي كالآتي:

أ. قرار الجمعية العامة للأمم المتحدة رقم 3314 لسنة 1974 بشأن تحديد الحالات التي تعد عدواناً وتسمح للدولة التي تتعرض لحالة منها، أن تستخدم حق الدفاع الشرعي الفردي والجماعي ضد الدولة المعتدية مضمون المادة 51 من ميثاق الأمم المتحدة.

ب. قرار الجمعية العامة للأمم المتحدة رقم 3034 لسنة 1972 الذي أدان الإرهاب وأوصى بالتمييز بين الإرهاب وبين حق الشعوب بتقرير مصيرها باستخدام الكفاح المسلح ضد الاستعمار وأنظمة التمييز العنصري وأنواع الهيمنة الأجنبية.

ج. قرار الجمعية العامة رقم 2770 لسنة 1973 الذي أفضى إلى تشكيل لجنة قانونية دولية تكلف بإعداد مشروع دولي لحماية الأشخاص المتمتعين بالحماية وفقاً لقواعد القانون الدولي، حيث تمت الموافقة على ميثاق منع ومعاقبة الجرائم ضد الأشخاص المتمتعين بالحماية الدولية بما في ذلك المبعوثين الدبلوماسيين بتاريخ 1983/9/14(فتلاوي، 2005، ص203).

د. قرار الجمعية العامة رقم 60/49 تاريخ 1996/2/17، والمتضمن الإعلان المتعلق بالتدابير الرامية إلى القضاء على الإرهاب الدولي.

الفرع الثاني: دور مجلس الأمن الدولي في مجال مكافحة الإرهاب

ويتمثل دور مجلس الامن فقط في القرارات الصادرة عنه، وبالرجوع إلى قائمة قرارات مجلس الأمن الدولي نجد أن هناك الكثير من القرارات التي تتعلق بالإرهاب ومكافحته وهي كالآتي:

أ. القرار 1999/1267 بشأن الحالة في افغانستان.

ب. القرار 2001/1373 الذي يعد أكثر القرارات شمولاً في تاريخ المجلس وأهمها على الاطلاق فيما يتعلق بمكافحة الإرهاب ويعتبر بجانب الاتفاقيات المتعلقة بالإرهاب أحد الدعائم التي يرتكز عليها النظام القانوني الدولي لمنع الإرهاب والقضاء عليه (خريسات، 2006/2005، ص53).

ج. القرار 2002/1390 بشأن الحالة في افغانستان، والقرار رقم 2003/1455 بشأن مكافحة الأخطار التي تهدد السلام والأمن الدوليين من جراء الأعمال الإرهابية، والقرار رقم 2003/1456 بشأن واجب الدول أن تكفل اتخاذ أي تدابير لمكافحة الإرهاب بما يتفق مع إلتزاماتها بموجب القانون الدولي.

د. قرار مجلس الأمن رقم 1999/1269 تاريخ 1999/10/19 والذي أشار إلى تزايد حالات الإرهاب الدولي الذي يعرض حياة الأفراد وأمن وسلامة الدول للخطر. ويلاحظ على القرار أنه لم يفرق بين العدوان والإرهاب..

ه. قرار مجلس الأمن رقم 1368 تاريخ 2001/9/12 وقراره رقم 1373 تاريخ 2001/9/28 وقد وضع القراران بعض المبادئ التي تتناقض مع ميثاق الأمم المتحدة، ومع مبادئ حقوق الإنسان، والإعلان العالمي لحقوق الإنسان، واتفاقية جنيف الثالثة بشأن أسرى الحرب لعام 1949، وبشأن قواعد تسليم اللاجئين السياسيين المعتمدة بين الدول وهذه المبادئ هي(فتلاوي، 2005، ص203):

1. اعتبر القرار هجمات برجي التجارة العالمية تهدد السلم والأمن الدوليين، ويشير مفهوم تهديد السلم والأمن الدوليين إلى الإنذار بوقوع حرب، فهل ما حصل في الولايات المتحدة الأمريكية يشير إلى ذلك؟ ثم أن مجلس الأمن لم يعتبر كثير من التهديدات بالحرب في كثير من المناطق مما يهدد الأمن والسلم والدوليين مثل الاعتداء والاحتلال الإسرائيلي لفلسطين.

2. يمنح القرار 1373 الولايات المتحدة حق الدفاع الشرعي، والدفاع الشرعي لا يتم إلا عند تعرض دولة للعدوان (م51 من ميثاق الامم المتحدة) وهذه الحالات كما سبق وأن أشـــرنا حددها القرار رقم 1974/3314 الصادر عن الجمعية العامة للأمم المتحدة ولم تتــضمن الأعمال الإرهابية لأن أعمال العدوان لا تصدر إلا من الدول.

3. يحمل القرار مسؤولية منع الهجمات الإرهابية على الدول كافة، علماً بأن غالبية الهجمات تصدر من أفراد وجماعات الى جانب الدول، بالتالي لا يمكن تحميل هذه الدول المسؤولية للدول لوحدها.

المطلب الثاني: جهود الدول في مكافحة الإرهاب التقليدي والإرهاب الإلكتروني

يمكن تناول الكثير من الجهود التي تبذلها الدول في مجال مكافحة الإرهاب والإرهاب الإلكترونـــي والجرائم الإلكترونية بصفة عامة، وتتناول الباحثة ذلك من خلال الحديث عن المعاهدات الدولية في هــذا الاطار في فرع، وفي فرع آخر تتناول الجهود الأخرى، كالآتي:

الفرع الاول: الاتفاقيات الدولية في مجال مكافحة الجرائم الإلكترونية

تتناول الباحثة في هذا المجال بعض الاتفاقيات الدولية في مجال مكافحة الإرهاب التقليدي والإرهاب الإلكتروني والجرائم الإلكترونية كالآتي:

أولاً: اتفاقيات مكافحة الإرهاب

وهذه الاتفاقيات هي:

أ. اتفاقية جنيف لمنع ومعاقبة الإرهاب لعام 1937، وتتعلق هذه الاتفاقية بالإرهاب الثوري فقط والاعتداءات الموجهة ضد سلطان الدولة (فتلاوي، 2005، ص202). وبمراجعة نصوص الاتفاقية نلاحظ أنها حثت الدول الأطراف على اتخاذ تدابير لمنع الإرهاب وبينت المادة الثانية منها الأعمال التي تكون جريمة إرهابية، حيث يشترط في العمل الإرهابي أن يكون من النوع الذي يدخل ضمن الأفعال الإجرامية الواردة في الاتفاقية والتشريعات العقابية الوطنية، وأن يوجه الفعل بطريقة مباشرة أو غير مباشرة إلى دولة، فالأفعال الموجهة ضد الأفراد لا تدخل في نطاق تطبيق الاتفاقية، وأن يكون الهدف من ارتكابه إحداث حالة من الفزع والرعب، وأن تتولد هذه الحالة لدى شخصيات معينة أو مجموعات معينة من الأشخاص، أو لدى الجمهور، وأن يدخل الفعل الإرهابي في عداد الأفعال الواردة في المادة الثانية من الاتفاقية، وأن يكتسب الفعل طابعاً دولياً.

ب. اتفاقية طوكيو لعام 1963، وتتعلق هذه الاتفاقية بالأعمال الإرهابية التي ترتكب على متن الطائرات وذلك بعد موجة خطف طائرات ولعدم وجود قواعد قانونية لتسوية المشاكل الناجمة عن

خطف الطائرات وتعيين الدولة المختصة بالنظر في جرائم الخطف هذه(فتلاوي، 2005، ص203).

ج. اتفاقية مكافحة الاستيلاء غير المشروع على الطائرات لعام 1970، فبعد موجة من عمليات خطف الطائرات وفشل بعض الدول في التوصل لحلول لمنع ذلك وعقد كثير من الاتفاقيات الثنائية، فقد جاءت هذه الاتفاقية لوضع القواعد القانونية التي تلزم الدول باتباعها في حالة التعرض لخطف طائرات أو في حالة الاستيلاء غير المشروع على الطائرات وباستخدام القوة أو التهديد بالقوة أو بأي شكل من أشكال التخويف بالاستيلاء على تلك الطائرات أو بممارسة السيطرة عليها أو بمحاولة القيام بأي عمل من هذه الأعمال(فتلاوي، 2005، ص204).

د. اتفاقية مكافحة الأعمال غير المشروعة المرتكبة ضد سلامة الطيران المدني لعام 1970(مونتريال)، واتفاقية منع أعمال الإرهاب ضد الأشخاص المتمتعين بحماية دولية وفقاً للقانون الدولي لعام 1973، والاتفاقية الأوروبية لقمع الإرهاب لعام 1977، وقد عقدت هذه الاتفاقية في إطار المجلس الأوروبي وتناولت الإرهاب الدولي. والاتفاقية الدولية لمناهضة أخذ الرهائن لعام 1979، واعلان الطيران المدني الدولي المكمل لاتفاقية مكافحة الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني لعام 1988 (مونتريال)، واتفاقية بحث الأعمال غير المشروعة الموجهة ضد سلامة الملاحة البحرية (روما) لعام 1988، والبروتوكول المتعلق بقمع الأعمال غير المشروعة الموجهة ضد سلامة المنشآت الثابتة الموجودة على الجرف القاري (روما) لعام 1988، واتفاقية تمييز المتفجرات البلاستيكية بغرض منعها (مونتريال) 1991 (فتلاوي، 2005، ص203).

ثانياً الاتفاقيات في مجال جرائم الانترنت وغسيل الأموال

حيث يتشابه ذلك مع أحكام جرائم الانترنت بما فيها الإرهاب الإلكتروني، كما أن غسيل الأموال يعد من الأنشطة الإرهابية سواء كانت تساهم أو تساعد في تنفيذ الأعمال الإرهابية الإلكترونيـــة أو التقليديـــة على السواء، أو يمكن الاستفادة منها في هذا المجال، وأهمها:

أ. اتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية لعـــام 1988 (اتفاقية فينا لعام 1988): وتضمنت أحكام هامة في مجال تجريم غـــسيل الأمـــوال والانـــشطة المصاحبة له كنقل الأموال وتحويلها، وتضمنت أحكام للتعاون الدولي وتجريم سلوكيات تنطـــوي على غسيل الأموال الناجم عن المخدرات(المادة الثالثة من الاتفاقية). وامتد نطاق التجريم ليشمل الممثلين والوسطاء والبنوك والمؤسسات المالية، وتوسعت في حماية الأمـــوال لتـــشمل الحقـــوق المادية وغير المادية(الخبيلي، 2006، ص94).

لكن يؤخذ على هذه الاتفاقية أنها تقتصر على غسيل الأموال الناتجة عن الاتجار بالمخدرات، لكن يمكن أن تؤسس انطلاقه لمكافحة هذه الجرائم، ومن جانب آخر يمكن الاســـتفادة مـــن الأحكـــام الواردة فيها في توجيه سلوكيات الدول وتوجهها نحو توسيع نطاق الحماية والتجريم في معاهدات أخرى للاستفادة منها في مجال تجريم أنشطة الإرهاب الإلكتروني خاصة أنشطة غسيل الأمـــوال عبر الإنترنت التي تعد المحرك الرئيسي للجرائم الإرهابية الإلكترونية.

ب. اعلان بازل لسنة 1988: حيث تضمن الاعلان توصيات رئيسية يتعين على المصرفيين اتباعهـــا

للسيطرة على ظاهرة غسيل الأموال ومنع االبنوك من تسهيل إخفاء الأموال أو تنظيفها، وبالمجمل جاء الاعلان لحماية المؤسسات المصرفية وابعادها عن الانشطة ذات الطبيعة الاجرامية (الخييلي، 2006، ص95).

ج. اتفاقية بودابست 2001 لمكافحة جرائم الانترنت وتهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الانترنت وبلورة التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها(الجنبيهي منير والجنبيهي ممدوح، 2005، ص180).

د. المعاهدة الاوروبية لمكافحة جرائم الانترنت: تتضمن بشكل رئيسي التزام الدول الأطراف فيها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبييانات وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر وصور القاصرين الاباحية وانتهاكات حقوق النسخ الرقمي (الجنبيهي منير والجنبيهي ممدوح، 2005، ص185-186).

الفرع الثاني: مظاهر تعاون الدول في التصدي للإرهاب التقليدي والإرهاب الإلكتروني

تبدأ هذه الجهود من خلال التشريعات الوطنية للدول حيث تقوم كل دولة بوضع التشريع اللازم لضبط التعاملات الإلكترونية، وعقاب المخالفين ومرتكبي الجرائم المعلوماتية. حيث أن هناك حاجة إلى التعاون الدولي المتبادل في مجال مكافحة جرائم الكمبيوتر، حيث تثور اشكاليات حول التحقيق في جرائم الكمبيوتر

أي مشكلات من الناحية القانونية من حيث بيانات الكمبيوتر والمعلومات المخزنة فيه واستخدامها في التحقيق. وتحديد معايير لوسائل الأمن المعلوماتي. اضافة للطبيعة العالمية لبعض جرائم الكمبيوتر. وأساليب الوقاية من جرائم الكمبيوتر والانترنت. وصعوبة التحقيق فيها من حيث عدم ارتباطها بالحدود الجغرافية، ولاستخدامها لتقنيات متطورة جداً. كما أن هناك حاجة لتطوير قدرات رجال الأمن والتحقيق في مجال جرائم الكمبيوتر، وتدريبهم على كيفية التعامل معها والوقاية منها، وكيفية التعامل مع مسرح الجريمة، واعطائهم الدورات اللازمة للتعامل مع معدات الحاسب الآلي والإلمام بالبرمجيات اللازمة للتشغيل لنشر الوعي بين أفراد الأجهزة الأمنية حول طبيعة هذه الجرائم من جانب وللمساعدة في الحصول على الأدلة الجرمية.

كما أن انتشار الجرائم الإرهابية وتعدد مجالاتها وصورها وطرق ارتكابها قد جعل الحاجة ملحة للتدخل الدولي والتعاون في مجال مكافحتها، من خلال ايجاد الآليات الأمنية اللازمة، وقد اتخذ التعاون الدولي مظهرين من النشاط هما: أنشطة لمنع الجرائم الإرهابية وأنشطة لمكافحتها.

أولاً: التعاون الدولي في مجال منع الجرائم الإرهابية

عقدت كثير من الاتفاقيات الدولية في هذا المجال ووضعت التزامات متعددة على الدول الأطراف منها: تبادل المعلومات حول الجرائم الإرهابية واتخاذ الإجراءات اللازمة ضدهم والمساعدة في إحباط العمليات الإرهابية(العفيف، 2011، ص243)، مثل اتفاقية نيويورك لحماية الأشخاص المتمتعين بحماية دولية لعام 1973، حيث جاء في المادة السادسة منها أنه لدى اقتناع الدولة الطرف التى يكون المظنون

بارتكابه الفعل الجرمى موجوداً فى إقليمها بوجود ظروف تبرر ذلك ، تعمد إلى اتخاذ التدابير المناسبة بموجب قانونها الداخلي لتأمين حضوره لغرض محاكمته أو تسليمه. ويجرى إبلاغ هذه التدابير دون تأخير سواء مباشرة أو بواسطة الأمين العام للأمم المتحدة إلى : الدولة التى ارتكبت فيها الجريمة، الدولة أو الدول التى يكون المظنون بارتكابه الفعل الجرمي من رعاياها أو الدول التي يقيم في إقليمها بصورة دائمة إن كان عديم الجنسية، الدولة أو الدول التى يكون الشخص المعني المتمتع بحماية دولية من رعاياها أو التي كان هذا الشخص يؤدى وظائفه باسمها، جميع الدول المعنية الأخرى، المنظمة الدولية التي يكون الشخص المعني المتمتع بحماية دولية من موظفيها أو معتمديها . وأنه يحق لأى شخص تتخذ بشأنه تلك التدابير: أن يتصل دون تأخير بأقرب ممثل مختص للدولة التى يكون هو من رعاياها أو الدولة التى تكون لها بوجه آخر أهلية حماية حقوقه أو إن كان عديم الجنسية فالدولة التي يطلب إليها حماية حقوقه وتكون هي مستعدة لحمايتها، وأن يزوره ممثل لهذه الدولة. كما أن غالبية الوثائق الدولية المعنية بالإرهاب تفرض التزاماً دولياً بالتعاون الأمني بين الدول وتقديم المساعدة المتبادلة.

ثانياً: التعاون الدولي في مجال مكافحة الجرائم الإرهابية

وهناك الكثير من الاتفاقيات الدولية في هذا المجال، ومن أهم أوجه التعاون التي جاءت بها:

أ. تسليم المجرمين: مثل اتفاقية لاهاي 1970 حيث أوجبت تسليم مختطفي الطائرات (المادة الثامنة منها). والاتفاقية الاوروبية لقمع الإرهاب 1977 (المادة الاولى والثانية منها).

ب. الاختصاص القضائي: أي الالتزام باحالة مرتكبي الجرائم الدولية إلى القضاء (المادة السابعة من اتفاقية لاهاي 1970).

ثالثاً: من التعاون الدولي دور الأجهزة الدولية والإقليمية في مجال غسيل الأموال، وأهمها:

أ. لجنة العمل المالي الدولية لمكافحة غسيل الأموال FATF التي تاسست عام 1989 خلال اجتماع القمة الاقتصادية الخامس عشر للدول السبع الصناعية، وتسهم هذه التوصيات برسم السياسة الجنائية في مجال غسيل الأموال من خلال تجريم غسيل الأموال وحث الدول على ذلك في تشريعاتها الوطنية، ورفع السرية عن أعمال البنوك، والتعاون في مجال الابلاغ عن الصفقات المشبوهة (الشوا، 2001، ص162. والخبيلي، 2006، 96).

ب. المنظمة الدولية للشرطة الجنائية (الانتربول): وتتعدد نشاطات هذه المنظمة بتعدد الجرائم وتلعب دوراً هاماً في مجال الجرائم الخطيرة كغسيل الأموال(الخبيلي، 2006، 97).

رابعاً: مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين الذي عقد في هافانا(هشام محمد فريد رستم، 2000، ص48-49):

أ. دعا الدول الأعضاء إلى أن تكثف جهودها في مجال مكافحة عمليات الإساءة في استعمال الحاسب الآلي خاصة فيما يتعلق بتلك التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني.

ب. جاء فيه الدعوة بالنظر إذا دعت الضرورة في:

1. تحديث الأنظمة والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن تكون الجزاءات بشأن سلطات التحقيق وقبول الأدلة على نحو ملائم .

2. النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة ، للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي .

ج. حث الدول الأعضاء على مضاعفة أنشطتها على الصعيد الدولي لمكافحة جرائم الحاسب الآلي والإنترنت، والانضمام للمعاهدات الدولية المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة في مجال هذه الجرائم.

د. حث مؤتمر الأمم المتحدة المتعلق بهذه الجرائم لفتح آفاق جديدة للتعاون الدولي في هذا المجال خاصة:

- وضع وتطوير معايير دولية لأمن المعالجة الآلية للبيانات
- وضع وتطوير تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية.
- وضع وتطوير اتفاقيات دولية جديد تتضمن أحكاماً تتعلق بتنظيم إجراءات التفتيش والضبط المباشر عبر الحدود على الأنظمة المعلوماتية، وكافة أشكال المساعدة المتبادلة، بشكل يكفل حماية حقوق الأفراد والدول وحرياتهم.

المبحث الثالث: الجهود الإقليمية والوطنية في مكافحة الإرهاب

لا تقف الجهود اللازمة لمكافحة الجرائم الإرهابية والجرائم الإلكترونية بما فيها الإرهاب الإلكتروني على الجهود الدولية على مستوى العالم بدوله وهيئاته، إنما يتعدى الأمر ذلك النطاق ليصل إلى مستويات إقليمية وعلى مستويات وطنية لفرادى الدول.

وحيث أن الباحثة تناولت في ما تقدم تلك الجهود الدولية وبعد أن استعرضت الصعوبات التي تقف أمام مكافحة هذه الجرائم فإنها في هذا المبحث تتناول الجهود على المستوى العربي والمستويات الوطنية لبعض الدول والمملكة الأردنية الهاشمية.

لذا تقوم الباحثة بتناول الموضوع في مطلبين:

المطلب الأول: الجهود الإقليمية العربية في مواجهة الإرهاب

المطلب الثاني: الجهود الوطنية للدول في مواجهة الإرهاب

المطلب الأول: الجهود الإقليمية العربية في مواجهة الإرهاب

أدركت الدول العربية أهمية التعاون الأمني لمواجهة كثير من الجرائم منها جريمة الإرهاب، خاصة في ظل تنامي القوى الإرهابية وتعزيز أنشطتها وتوسيع نطاق عملياتها الإرهابية، حيث أصبح من الصعب على دولة واحدة مواجهة الخطر الإرهابي، مما حتم تعميق سياسة التكامل الأمني، ومن صور التعاون العربي:

أولاً: الاتفاقية العربية لمكافحة الإرهاب لعام 1988

وقد اعتمدت من قبل مجلس وزراء الداخلية والعدل العرب في دورة انعقاد خاصة عام 1998 لبحث سبل مواجهة الإرهاب ومهددات الأمن والسلم العربي ومواجهة الجماعات الإرهابية بجهد مشترك، وتكونت الاتفاقية من 42 مادة تتلخص مظاهر مكافحة الإرهاب وجهوده فيها بما يأتي(العفيف، 2011، ص265-266):

أ. تعزيز التعاون بين الدول العربية لمكافحة الإرهاب والجرائم الإرهابية.

ب. التاكيد على الالتزام بالمبادئ الأخلاقية والدينية السامية لاسيما أحكام الشريعة الاسلامية.

ج. التمييز بين الإرهاب وبين الكفاح الوطني وحق الشعوب بالكفاح ضد الاحتلال الاجنبي والعدوان بمختلف وسائل الكفاح والسعي نحو التحرير وتقرير الحق بالمصير والحفاظ على الاستقلال والوحدة لكل بلد عربي. وبالتوافق مع مقاصد ومبادئ الامم المتحدة.

د. منع تقديم المساعدة المالية أو العينية للتنظيمات الإرهابية أو استقبالها على أراضيها أو إيوائها أو إعداد المعسكرات لتدريبها أو تسليحها أو تمويلها ومساعدتها.

ه. اتخاذ تدابير أمنية لمنع الجرائم الإرهابية: حيث نصت المادة الثالثة منها على نوعين من التدابير: تدابير المنع وتدابير القمع:

1. اتخاذ تدابير المنع وهي:

- تعديل التشريعات الوطنية للدول بما يتفق مع الاتفاقية وقد سلك المشرع الأردني ذلك في قانون العقوبات حيث أدخل الجرائم الإرهابية في نطاق التجريم ووضع تعريفاً للإرهاب.
- أكدت الاتفاقية على التعاون والتنسيق بين الدول المتعاقدة لمكافحة هذه الجرائم.
- التعهد بتطوير وتعزيز أنظمة الكشف عن نقل وتصدير وتخزين واستخدام الأسلحة والذخائر والمتفجرات ووسائل القتل والتدمير وإجراءات مراقبتها عبر الحدود ومنع انتقالها للاغراض غير المشروعة
- تعزيز نظم حماية وتأمين المنشآت ووسائل النقل العام وحماية أمن وسلامة الشخصيات والبعثات الدبلوماسية والقنصلية والمنظمات الدولية والإقليمية
- تعزيز أنشطة الإعلام الأمني وتنسيقها بين الدول لكشف وفضح أهداف الجماعات والتنظيمات الإرهابية

- أن تلتزم كل دولة وتتعهد بإنشاء قاعدة بيانات لجمع وتحليل المعلومات الخاصـــة بالعناصـــر والجماعات الإرهابية ومتابعة المستجدات

2. تدابير المكافحة وهي:

- الالتزام بالقبض على مرتكبي الجرائم الإرهابية ومحاكمتهم وفقاً لأحكام القانون
- تأمين حماية فعالة للعاملين في ميدان العدالة الجنائية
- تأمين حماية فعالة لمصادر المعلومات عن الجرائم الإرهابية والشهود فيها
- توفير المساعدة اللازمة لضحايا العمليات الإرهابية
- التعاون الفعال بين الأجهزة

3. التعاون في المجال القضائي(المواد من من 13-18):

- في مجال تسليم المجرمين (المادة الخامسة والمادة السادسة والثامنة منها).
- في مجال الإننابة القضائية: اجازت الاتفاقية العربية لكل دولة متعاقدة أن تطلب إلـــى دولـــة أخرى متعاقدة القيام في اقليمها بالاجراءات الجنائية نيابة عنهـــا (المـــادة التاســـعة والمـــادة العاشرة).

ثانياً: الاتفاقية الخاصة أو ميثاق الشرف أو مدونة سلوك الدول الأعضاء لمكافحة الإرهـــاب، والتـــي اعتمدها مجلس وزراء الداخلية العرب عام 1996 بقراره رقم 257 د 1996/13 حيث أكدت الدول العربية التزاماتها الدينية والأخلاقية والإنسانية التي تعتنقها وتراثها الحضاري وتقاليدها الراسخة التي تدعو إلى نبذ كافة أشكال الإرهاب الذي يهدد أسس الشرعية وسيادة القانون (الأمانة العامة لمجلـــس وزراء الداخلية العرب، 1996، ص2). وتضمنت هذه المدونة معالم رئيسية لمكافحة الإرهاب تتمثل بـــ:

أ. ادراك الدول لما يحقق التعاون بينها في المجالات الأمنية والدفاع عن الـــصورة الحقيقـــة للعروبة والاسلام.

ب. إدانة كافة أعمال الإرهاب أياً كان مصدره أو سببه أو غرضه والالتزام بعـــدم القيـــام أو الشروع أو الاشتراك بأي صورة من صور الأعمال الإرهابيـــة والحيلولـــة دون اتخـــاذ أراضيها كمسرح للتخطيط أو لتنفيذ العمليات الإرهابية.

ج. التعهد بالتضييق على العناصر الإرهابية ومنع تسللها عبر حدودها وإقامتها على أراضيها.

د. التعهد بعدم ايواء الإرهابيين أو تدريبهم أو تسليحهم أو تمويلهم وتمويل أعمالهم.

ه. تقديم المساعدة المتبادلة في مجال إجراءات التحري والقبض على الأشـــخاص الهـــاربين المتهمين أو المحكوم عليهم بجرائم إرهابية وتعزيز الأنشطة الإعلامية لإبـــراز الـــصورة الحقيقية للدين الاسلامي والتصدي للحملات المغرضة التي تنال من الدين الاسلامي ومن

عروبة الأمة العربية والعمل على كشف مخططات التنظيمات والجماعات الإرهابية وخطورتها.

ثالثاً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 لأهمية تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها ولتبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي من هذه الجرائم (محمد الدغيلبي، 2012، بدون رقم صفحة).

رابعاً: على مستوى وزراء الداخلية العرب تم إقرار الاستراتيجية العربية الأمنية بتاريخ 1983/2/7 التي تهدف إلى حماية المجتمع العربي من الإرهاب، (العفيف، 2011، ص263). ومن الجريمة بكافة أنواعها وأشكالها خاصة غسيل الأموال حيث تضمنت الدعوة لاتخاذ تدابير قانونية وادارية مناسبة لمساعدة الأجهزة المختصة في تتبع وتجميد ومصادرة الأموال المتأتية من الاتجار غير المشروع بالمخدرات والعمل على توعية المواطنين والشركات الاستثمارية بالأساليب التي يمكن استخدامها من قبل عصابات التهريب واغرائهم في عمليات غسيل الأموال(الخبيلي، 2006، ص97).

خامساً: الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب لسنة 2012 لخطورة ما ينجم عن غسل الأموال وتمويل الإرهاب من مشاكل ومخاطر تقوض خطط التنمية الاقتصادية وتعرقل جهود

الاستثمار وتهدد الاستقرار السياسي والاقتصادي والأمني وتخل بسيادة القانون فضلاً عن أن هذه الأفعال تعد جرائم عبر وطنية تمس كل البلدان واقتصادياتها مما يستلزم التعاون على الوقاية منها ومكافحتها. وفي الأردن جرت المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 والذي يأتي التزاماً بالمادة 33 من الدستور ولأهمية تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات. والتصديق على الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب لسنة 2012 والذي ياتي التزاما بنص المادة 33 من الدستور ونظراً لخطورة ما ينجم عن غسل الأموال وتمويل الإرهاب من مشاكل ومخاطر تقوض خطط التنمية الاقتصادية وغيرها من آثار (مجلس الوزراء يوافق على اتفاقية مكافحة غسل الأموال وتمويل الإرهاب لسنة2012، خبر منشور في موقع محطة الحقيقة الدولية، بدون رقم صفحة).

سادساً: مؤتمرات القمة العربية التي تطرقت لخطر الإرهاب والحاجة للتعاون العربي في الحد من انتشاره كمؤتمر القمة العربية في الدار البيضاء عام 1985 ومؤتمر عمان عام 1987 ومؤتمر بيروت 2002(العفيف، 2012، ص263).

المطلب الثاني: الجهود الوطنية للدول في مكافحة الإرهاب

يمكن تطبيق ذات الوسائل المستخدمة في علاج الإرهاب الإلكتروني والارهاب التقليدي في مكافحة كلا النوعين من الإرهاب مع فارق الخصوصية الذي يتمتع به الفضاء الإلكتروني. ومن هنا تتناول الباحثة التطبيقات العملية التي قامت بها الدول في مجال مكافحة الإرهاب بصورتيه. ففي الدول المتقدمة تنبه الغرب لقضية الإرهاب الإلكتروني ومخاطره، فقام الرئيس الأمريكي بيل كلينتون عام 1996 بتشكيل لجنة لحماية منشآت البنية التحتية الحساسة (www.nipc.gov)، والتي أقرت بأن مصادر الطاقة الكهربائية والاتصالات وشبكات الكمبيوتر تعد ضرورية لنجاة الولايات المتحدة، وأنها ستكون الهدف الأول لأية هجمات إرهابية محتملة قد تستهدف أمن الولايات المتحدة، فقامت الوكالات الحكومية بإنشاء هيئات ومراكز خاصة للتعامل مع احتمالات الإرهاب الإلكتروني مثل إنشاء مركز حروب المعلوماتية التابع لوكالة الاستخبارات المركزية. ووافق ذلك خطوات على المستوى الأوروبي حيث قامت قوات الأمن التابعة لحلف الأطلسي، باتخاذ إجراءات مماثلة للإجراءات المتخذة في الولايات المتحدة (ويكيبيديا الموسوعة الحرة، بدون رقم صفحة).

في أمريكا هناك حماية جيدة ضد الاعتداءات التي تتم عن طريق الانترنت، حيث هناك اهتمام بتأمين أنظمة الكمبيوتر الحكومية ضد الاعتداءات الإرهابية على أمريكا، وهناك مكتب خاص يعرف بالمكتب الاتحادي للأمن وتكنولوجيا المعلومات الذي يركز بشكل خاص على كل ما يتعلق بتأمين البنية التحتية لتكنولوجيا المعلومات.

وهناك بعض المشاريع المشتركة كمشروع (ايشلون) الذي أقيم بالاشتراك مع دول أوروبية للتجسس على رسائل الانترنت والمكالمات الهاتفية في العالم، ومشروع كارنيفور، وظهر نتيجة لذلك تشابك في الصلاحيات لأن الـــ (اف بي آي) واستخبارات الجيش مكلفان بمتابعة التهديدات الداخلية فيما

تعمل الـــ"سي أي اي" في مواجهة القضايا الخارجية. وهذا ما أدى إلى انتشار المجموعات المتخصصة بمكافحة الإرهاب الإلكتروني في أجهزة الأمن المختلفة. ويختص الـــ(اف. بي آي) حالياً بملاحقة المخترقين (هاكرز)، وتقوم أجهزة الخدمات السرية بملاحقة الإرهاب الرقمي في حالات الصيرفة الإلكترونية والنصب والاحتيال والتنصت، ويقوم سلاح الجو الذي قام بتأسيس (فرق هندسة الأمن الإلكتروني) بمهمة محاولة اختراق أنظمة وشبكات عسكرية حول العالم(الصيفي، 2008، بدون رقم صفحة).

وفي مجال الارهاب الالكتروني هناك بعض المظاهر لمكافحته كالآتي (الصيفي، 2008، بدون رقم صفحة):

- في اليابان وبعد اختراقات عديدة لأنظمة الكمبيوتر الحكومية، وتمكن المخترقون من الـــدخول إلـــى أجهزة الموقع الحكومي الياباني ومحو بيانات مهمة تتضمن إحصاءات عن عدد السكان عنها، وتمكن المخترقون من نشر رسائل تنتقد الموقف الياباني الرسمي من مذابح نانكين التي يتهم بارتكابها الجنود اليابانيون في الصين عام 1937 على موقع وكالة التنسيق والادارة ووكالـــة العلـــوم والتكنولوجيـــا، وظهور بعض حالات من الإرهاب الرقمي، لذا دعت الحكومة إلى التصدي لخطر الإرهاب الرقمـــي بمختلف الوسائل والأساليب اللازمة.
- عربياً: يشير بعض الخبراء الاستراتيجيين (كالعراقي مصطفى العاني/ من مركز الخليج للأبحاث) إلى أن هناك الكثير من التحويلات المالية التي تحصل للجماعات الإرهابية بطرق إلكترونية، كما أن هناك عمليات تبادل للمعلومات حول العمليات الإرهابية وكيفية الحصول على صـــناعة القنابـــل، وتجنيـــد العناصر، والتشجيع على العمليات الإرهابية، والدعاية لها عبر الإنترنت. الا أن أجهزة الاستخبارات

العربية أنفقت ملايين الدولارات لتعقب وتحليل المواقع الإلكترونية التي تتم من خلالها هذه العمليات واغلاقها. وأن هناك حرباً هجومية ودفاعية قائمة بين أقسام متخصصة تابعة للأجهزة الأمنية العربية وتلك المواقع الإرهابية.

- في اسرائيل قام رئيس الوزراء الإسرائيلي بتشكيل فريق لمكافحة الإرهاب الإلكتروني برئاسة الميجور جنرال احتياط اسحاق بن اسرائيل، رئيس وكالة الفضاء الإسرائيلة والمجلس الوطني للبحوث والتنمية، لوضع استراتيجة خاصة بمواجهة مخاطر الحرب الإلكترونية المحتملة ضد إسرئيل، ويضم الفريق عناصر تابعة للموساد، والمخابرات العسكرية، وجهاز الأمن العام (الشاباك)، وخبراء ومتخصصين في علوم الكمبيوتر وحرب الفيروسات الإلكترونية، وممثلين عن الهيئات الحكومية، ووزارة العلوم والبحث العلمي وكتب مكافحة الإرهاب. وقد تم تشكيل هذا الفريق عقب ظهور ما يسمى بفيروس (الستكسنت) الذي أضر بشبكة الحاسب الآلي في المفاعلات النووية الايرانية. وتاتي هذه الجهود لتحديد المطلوب من الحكومة الاسرائيلية القيام به في مجال حرب الفيروسات الإلكرتونية. علما بأن إسرائيل لديها العديد من الهيئات واللجان المتخصصة في الحرب الإلكترونية الدفاعية أو الهجومية مثل هيئة "تهيلا" الحكومية التي تم تأسيسها عام 1997 وتتبع وزارة المالية، وعدة هيئات في وحدات جيش الإحتلال الإسرائيلي كالموساد والمخابرات الحربية والشاباك، وهيئة الحرب الإلكترونية التابعة للوحدة رقم 8200 في المخابرات العسكرية (عمرو عطية، **د.س،** بدون رقم صفحة).

الفصل الخامس

الخاتـــــــــمة والتوصيات

أولاً: الخاتمة

أصبح الإرهاب الإلكتروني خطراً عارماً يهدد ويخيف العالم بأسره، وأصبح العالم عرضة للهجمات الإرهابية عبر الإنترنت، ومن أي مكان في العالم، وأصبحت هذه المخاطر الكبيرة تتفاقم وتزداد كل يوم، وباتت التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية، لذا فقد سعت العديد من الدول إلى اتخاذ تدابير لمواجهة الإرهاب الإلكتروني. وقد توصلت الباحثة من خلال الدراسة إلى النتائج الآتية فيما يتعلق بموضوع الدراسة:

أولاً: أن الإرهاب الإلكتروني ما هو الا صورة من صور الإرهاب التقليدي، وأن تعريف الإرهاب قد مر ضمن كثير من المحاولات وكثير من المعايير، وللاهواء السياسية، خاصة للدول الكبرى، وقد وضعت له عدة تعريفات، وتطرقت له الشريعة الاسلامية وعرف أيضاً على المستوى العربي والمستوى الوطني والدولي وتعرضت للتعريف أيضاً الهيئات الدولية كالامم المتحدة، وفي الاتفاقيات الدولية، ووضع اتفاقيات خاصة بشأنه. وتبين بالمحمل أنه عبارة عن استراتيجية عنف محرم دولياً، تحفزها بواعث عقائدية (آيديولوجية)، وتتوخى إحداث رعب داخل شريحة خاصة من مجتمع معين، ويتم من قبل الدول، أو من قبل الجماعات بمساندة الدول معينة، لتحقيق أهداف سياسية واستراتيجية، من خلال ممارسة أفعال خارجة على القانون، تستهدف خلق حالة من الذعر الشامل في المجتمع.

ثانياً: أن للإرهاب ثلاثة أنواع: الإرهاب ضد النظام القائم للإطاحة به، وإرهاب الدولة، والإرهاب الذي تمارسه منظمات التحرير الوطنية عند عجزها عن شن حرب واسعة النطاق. وبالمقابل كان هناك تقسيم آخر يقسم الإرهاب إلى نوعين هما: الإرهاب التقليدي، والإرهاب الإلكتروني. ومن حيث مرتكب الجريمة تبين أن الإرهاب نوعين هما: إرهاب الدولة، وإرهاب المنظمة أو الجماعة.

ثالثاً: أن للإرهاب أسباب بشكل عام وتوصلت إلى أنها: أسباب سياسية أو اقتصادية أو اجتماعية، أو انتكاك حقوق الإنسان، أو تدمير البيئة. اضافة إلى بعض المؤثرات الخاصة المرتبطة بهذه الأسباب، والفراغ الفكري، والتطورات العلمية والتكنولوجية، وثورة الحاسوب والاتصالات والإنترنت، وما سببته من تطورات في مختلف المجالات.

وأن له أساليب وأشكال هي: حرب العصابات، والاغتيالات السياسية، واحتجاز الرهائن، وخطف الطائرات، وضرب المدنيين بالقنابل، واحتجاز السفن، والاستعمار الاستيطاني، واحتلال الأراضي والتوسعة الإقليمية. وتوصلت الدراسة في هذا الصدد أن الإنترنت أو الفضاء الإلكتروني يمكن أن يكون وسيلة للقيام بكافة هذه الصور، بما في ذلك الاغتيال والاستعمار. كما قد يكون الإنترنت ذاته هدفاً للعمليات الإرهابية، لتدمير بنية المعلومات لدى جهة معينة.

رابعاً: أن هناك علاقة بين الفضاء الإلكتروني والجريمة المعلوماتية بالإرهاب من حيث أثر التكنولوجيا الحديثة في الأمن الوطني، والتعريف بصور الجرائم المعلوماتية التي يعد الإرهاب الإلكتروني أحدها، ومن حيث الربط بين الفضاء الإلكتروني والجرائم الإرهابية. فالفضاء الإلكتروني يلعب ثلاثة ادوار في ذلك فقد يكون هدف الجريمة، وقد يكون وسيلة ارتكابها، وقد يكون بيئة ارتكاب الجرم. وهذه الادوار تسببت في تعدد صور الجرائم الإرهابية الإلكترونية، فكان منها ما هو اعتداء على الأشخاص والأموال، ومنها ما يتعلق بالدخول غير المصرح به، ومنها جرائم تساعد في تحقيق جرائم الإرهاب الإلكتروني أو ترافقها، وقد توقفت الباحثة على معالجة المشرع الأردني لهذه الصور ضمن التشريعات ذات الشأن.

خامساً: أن الإرهاب الإلكتروني يعد نوعاً من أنواع الجرائم المعلوماتية، حيث يتخذ الفضاء الإلكتروني صورة المجال أو النطاق الذي يمارس به العمل الإرهابي، أو الوسيلة التي يتم من خلالها ممارسة العمل الإرهابي، فقد يستخدم الانترنت كما اوضحت الدراسة في الوظيفة الاعلامية للجماعات الإرهابية، أو للاتصال والتنسيق، أو كوسيلة لتحقيق الأهداف الإرهابية، أو للتعليم والتدريب.

سادساً: أن للإرهاب الإلكتروني: جانب مادي يتعلق بالمواد التي يستخدمها الإرهاب أو الإرهابي للنقـل والاتصال أو الأسلحة المستخدمة سواء كانت أسلحة خفيفة أو متفجرات أو أسلحة كيميائيـة وبيولوجيـة. وجانب معنوي يتعلق بالمعارف والخبرات والمهارات والأساليب اللازمة لتعامل الإرهـابي مـع البيئـة المحيطة، واستخدام أو تصنيع الجانب المادي من تكنولوجيا الإرهاب.

سابعاً: أن أسباب الإرهاب الإلكتروني تتشابه مع أهداف وأسباب الإرهاب التقليدي، الا أنه نـشأ بـسبب ظهور التقنية الإلكترونية، وشجع عليه صعوبة الرقابة على الانترنت أو المحاسبة على ما ينشر فيه.

ثامناً: أن أركان جريمة الإرهاب الإلكتروني هي نفس أركان جريمة الإرهاب العادية، مع تميزهـا مـن حيث الأداة الجرمية، وهي: المواقع الإكترونية، والفيروسات والدودة والقنابل الإلكترونية والقرصنة.

تاسعاً: أن جريمة الإرهاب الإلكتروني من الجرائم العمدية فلا يمكن تصور وقوع الجريمة بخطأ، إلا انها قد تكون قصد عام أو قصد خاص.

عاشراً: توصلت الدراسة إلى الجهود التي بذلت في مكافحة الإرهاب الإلكتروني، حيث تعرفـت علـى الجهود الحثيثة والمستمرة لمكافحة خطر الإرهاب الإلكتروني على كافة المستويات وفي كافة المجالات، بالرغم من أن بعض الجهود أو اغلبها ينصب في اطار مكافحة الإرهاب بشكل عام دون تحديد أو تمييز بين الإرهاب الإلكتروني أو الإرهاب بمفهومه التقليدي، الا أن مثل تلك الجهود تنطبق بالفعل على كـلا الصورتين، وقد توصل هذا الفصل إلى أنه هناك مجموعة من الصعوبات في مجال مكافحـة الإرهـاب والإرهاب الإلكتروني، وقد بينت الدراسة وتوصلت إلى التدابير اللازمة لمكافحة ومقاومة هذه الصعوبات، ثم أوضحت الدراسة مجموعة الجهود الدولية والإقليمية والوطنية في مجال مكافحة الإرهاب والإرهـاب الإلكتروني.

حادي عشر: أن هناك صعوبات تواجه عملية مكافحة الجرائم المعلوماتية مثل: سهولة إخفاء الجريمة، ونقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في مجال التكنولوجيا والفضاء الإلكتروني، وصعوبة الوصول إلى مرتكبي أغلب الجرائم المعلوماتية لسهولة اختبائهم وعدم كشف هوياتهم. ومنها صعوبات تواجه التعاون الدولي في هذا المجال كعدم وجود اتفاق عام مشترك بين الدول حول الأفعال الجرمية، واختلاف مفاهيم الجريمة باختلاف الحضارات، وعدم وجود معاهدات دولية لمواجهة المتطلبات الخاصة بالجرائم الإرهابية الإلكترونية، ووجود عوائق ومشكلات قانونية وفنية فيما يتعلق بالقيام ببعض إجراءات التحقيق وتعقب وملاحقة مرتكبي هذا النوع من الجرائم، مثل التفتيش والانابة والاختصاص. اضافة إلى بعض الصعوبات في مجال الإثبات في هذه الجرائم كطبيعة الدليل وصعوبة الوصول إليه وسهولة محوه.

ثاني عشر: أن هناك تدابير لمكافحة الإرهاب توصلت اليها الباحثة وقامت بتقسيمها إلى قسمين رئيسيين هي تدابير عادية منها ما هو من تدابير ووسائل المنع، ومنها ما يتعلق بالقمع. وهناك تدابير فنية إلكترونية خاصة بطبيعة الجريمة الإرهابية الإلكترونية منها: المقاومة الفنية البحتة كتشفير البيانات وأنظمة الحماية الإلكترونية وبرامج الكشف عن الفيروسات، وعدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية، وعمل وسائل التحكم في الدخول إلى المعلومات والمحافظة عليها، وتوزيع مهام العمل بين العاملين. وهناك المقاومة الفنية النظامية كمراقبة الإنكشافات، وإيجاد الثغرات في الحاسب والشبكات، وانشاء ادارات متخصصة في هذا المجال.

ثالث عشر: أن هناك جهود لمكافحة الإرهاب والإرهاب الإلكتروني، من قبل الأمم المتحدة، والدول منها ما يصب في باب الاتفاقيات الدولية في مجال مكافحة الجرائم كاتفاقيات مكافحة الإرهاب والاتفاقيات في مجال جرائم الانترنت وغسيل الأموال، ومنها ما يتعلق بالجهود العملية لتعاون الدول في التصدي للإرهاب والإرهاب الإلكتروني في مجال تسليم المجرمين، والاختصاص القضائي.

ثانياً: التوصيات

توصي الباحثة بما يأتي:

أولاً: اتخاذ إجراءات تشريعية تتماشى مع الجرائم الإلكترونية تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم سواء ما تعلق منها بالقواعد الموضوعية، أو القواعد الشكلية، لاسيما في مجال الدليل والإثبات والاختصاص وإجراءات التعاون وقواعد الإجراءات الجنائية.

ثانياً: وضع التشريعات اللازمة لمواجهة هذا التنوع من الجرائم من خلال نصوص التجريم للتوافق مع مبدأ المشروعية الذي يقضي بألا جريمة ولا عقوبة الا بنص.

ثالثاً: ضرورة التنسيق والتعاون بين الدول على المستويات الإقليمية والدولية من النواحي القضائية والإجرائية.

رابعاً: التعاون الدولي في مجال مكافحة هذه الجرائم من حيث: مواكبة التطور الحاصل في مجال التكنولوجيا الحديثة خاصة ارتكاب هذا النوع من الجرائم، ووضع الأحكام القانونية اللازمة لضبط التعاملات الإلكترونية، ومكافحة الجرائم المعلوماتية، والتفتيش والتحقيق وغيرها.

خامساً: ضرورة تخصيص إدارات خاصة ومستقلة لمكافحة الجرائم المعلوماتية والتعامل معها، ورفدها بأشخاص مدربين ويتمتعون بالخبرة في المجال الإلكتروني والشرطي على السواء.

سادساً: تدريب القضاة وأعضاء سلطات التحقيق بشأن التعامل مع أجهزة الحاسوب الآلي والإنترنت.

سادساً: تطوير وبناء قدرات أجهزة الأمن والأجهزة المهنية بالتعامل مع الجرائم الإلكترونية، خاصة الإرهابية منها، من خلال التدريب على مختلف الأنشطة، وطرق المكافحة بما في ذلك أساليب الوقاية منها وإجراءات الكشف المبكر عنها، والتعامل مع مسرح الجريمة، والتحقيق فيها.

سابعاً: وضع الآليات اللازمة لمراقبة المواقع وانشائها وتنظيم ذلك، خاصة تلك المواقع التي تستخدم لنشر الأفكار السامة والهدامة التي تخدم الأغراض الإرهابية وتعلم الإرهاب والوسائل المساعدة له. وحجب

المواقع التي يشتبه بانها تتبع لجماعات إرهابية أو أنها ذات ميول إرهابية أو تخدم أغراض الجماعات الإرهابية بطرق مباشرة أم غير مباشرة.

ثامناً: إتاحة الفرصة للمواطنين للمشاركة في مكافحة الجرائم المعلوماتية بما فيها الإرهاب الإلكتروني من خلال إيجاد خط للتواصل مع الجهات المعنية للابلاغ عن هذه الجرائم

تاسعاً: المساهمة في نشر الوعي المتعلق بجرائم الإرهاب عامة وجرائم الكمبيوتر خاصة بين صفوف المواطنين، ونشر الوعي المجتمعي المتعلق بالمخاطر النفسية والاجتماعية الناجمة عن الاستخدامات غير الآمنة للانترنت

عاشراً: تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم الإرهابية والجرائم المعلوماتية والدخول في الاتفاقيات الدولية الخاصة بذلك

حادي عشر: وضع الآليات اللازمة للحد من استخدام وسائل التكنولوجيا الحديثة وتطبيقات الانترنت في تنفيذ العمليات الإرهابية الإلكترونية. ووضع الآليات اللازمة للحد ممن الاختراقات التي تتم للخصوصية عبر الانترنت كاختراق البريد الإلكتروني وهتك حرمة المعلومات والبيانات وتدميرها.

ثاني عشر: الاهتمام بالجانب القانوني لهذه الجرائم والتعامل معها ودراستها إلى جانب الاهتمام الفني. مثل تشجيع الأبحاث والدراسات في هذا المجال.

ثالث عشر: في ضوء القصور التشريعي في مجال الإرهاب الالكتروني، وبالرغم من مواكبة المشرع الاردني وتقديمه لنظام من الحماية لتكنولوجيا المعلومات فإنه بصرف النظر عن مدى كفايته فإن الباحثة توصي بالاهتمام بجانب الارهاب الالكتروني من خلال تقديم أفضل حماية ممكنة وذلك من خلال الاجراءات الآتية:

- تعديل قانون العقوبات وتحديداً النصوص المتعلقة بالارهاب التقليدي والتي من الممكن اعتبارها كافية لمعالجة الجريمة الارهابية التقليدية، من خلال مد حماية هذه النصوص لتشمل الارهاب الالكتروني دون الخوض بتعريف محدد للارهاب الالكتروني انما فقط من خلال تبيان وتوضيح مفهومه من حيث

النطاق أنه يشمل الارهاب الذي يقع على أهداف ووسائل الكترونية او معلوماتية أو الارهاب الذي يتم من خلال هذه الوسائل، بالتالي يمكن تطبيق الاحكام المتعلقة بجريمة الارهاب التقليدي على كافة صور الارهاب.

- تعديل التشريعات القائمة التي تعالج الجرائم المعلوماتية من خلال اما الاحالة لقانون العقوبات بالنسبة لجريمة الارهاب الالكتروني على فرض تعديله، او من خلال افراد نصوص واحكام خاصة بهذا النوع من الارهاب من حيث الركن المادي والعقوبة، ليشمل الركن المادي كافة الصور الممكنة لهذا النوع من الارهاب سواء من حيث النشاط او من حيث الاداة والوسيلة التي يتم من خلالها او من حيث الفعل المكون للركن المادي لها.

- توحيد صور التجريم المتعلق بالارهاب الالكتروني في قانون واحد والافضل قانون جرائم أنظمة المعلومات، والتوصية في التشريعات الالكترونية الاخرى التي تعالج انواع وحالات خاصة من الاعتداءات الالكترونية الى هذه القانون.

- من الحلول الممكنة ايجاد نص قانوني عام في قانون العقوبات او في قانون جرائم انظمة المعلومات يتعلق بالارهاب الالكتروني ومفهومه بشكل عام، والاحالة فيما يتعلق بالركن المادي له الى النصوص المتفرقة في التشريعات الاخرى. اي ان يعاقب على هذه الافعال بعقوبة تختلف عن العقوبة المقررة لها في تلك النصوص متى ارتبطت مع مفهوم الارهاب الالكتروني في هذا النص العام. وربما تكون هذه الطريقة افضل لعدم امكانية المشرع التنبؤ بالافعال التي قد تحدث مستقبلا والتي قد تدخل في باب الارهاب دون ايجاد نص يجرمها فنكون امام قصور ومعالجة تشريعية.

ويمكن ان اقترح على المشرع النصوص الآتية أسوة بالمشرع الفرنسي:

- تعريف الأعمال الإرهابية أنها الأعمال ذات علاقة بمشروع فردي أو جماعي يهدف إلى الاخلال بشكل خطير بالنظام العام بالترويع أو بالرعب، كالأعمال الإجرامية الآتية: ...، السرقة، الابتزاز، التدمير، التجريد، الاتلاف، وكذلك الجرائم في مجال المعلوماتية.

- تجريم محو وتعديل البيانات المعالجة آلياً أو التدخل في طرق معالجتها، وتعطيل أو افساد تشغيل نظام المعالجة الالية للبيانات.
- تعريف الارهاب الالكتروني بأنه تلك الاعمال التي تمثل عدواناً على نظم المعالجة الآلية للبيانات متى حدثت وارتكبت بشكل يمثل اخلالاً كبيراً وخطيراً بالنظام العام سواء ارتكبهــا أفــراداً طبيعيــين أو أشخاص معنويين.

المراجع العربية:

الكتب العامة

1. ابراهيم، خالد ممدوح (2009)، الجرائم المعلوماتية، الاسكندرية: دار الفكر الجامعي.
2. أحمد، هلالي عبد اللاه(1997)، تفتيش الحاسب الآلي وضمانات المتهم المعلوماتي، ط1، القاهرة: دار النهضة العربية.
3. اسماعيل، عزت(1996)، الإرهاب والقانون الدولي، القاهرة: دار الفكر العربي.
4. البداينة، ذياب(2002)، الأمن وحرب المعلومات، عمان: دار الشروق للنشر والتوزيع.
5. بن محمد سفر، حسن(د.س)، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، الدكتور، بحث مقدم لمجمع الفقه الإسلامي الدولي.
6. بن يونس، عمر(2004)، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس.
7. بهنام، رمسيس(2008)، الجرائم المضرة بالمصلحة العمومية، الاسكندرية: منشأة المعارف.
8. بوادي، حسنين المحمدي(2004)، تجربة مواجهة الإرهاب، ط1، الاسكندرية: دار الفكر الجامعي.
9. بولتز، فرانك، وج ب دونيس، كينيث، وشولتز، داقين. ب (1999)، أسس مكافحة الإرهاب، ج1، ترجمة: الحناوي، هشام، ط1، القاهرة: المكتب العربي للمعارف.
10. التل، أحمد(1998)، ط1، الإرهاب في العالمين العربي والغربي، عمان.
11. تمام، أحمد حسام طه(2000)، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية)، ط1، القاهرة: دار النهضة العربية.
12. الجبور، محمد(1993)، الجرائم الواقعة على أمن الدولة في القانون الأردني والقوانين العربية، ط1، عمان.

13. الجنبيهي، منير محمد، و الجنبيهي ممدوح محمد(2006)، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، الإسكندرية: دار الفكر العربي.

14. حجازي، سهير حجازي(د.س)، التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، دولة الإمارات العربية المتحدة، العدد91.

15. حجازي، عبد الفتاح بيومي(2002)، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، الاسكندرية: دار الفكر الجامعي.

16. حجازي، عبد الفتاح(2009)، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات، ط1، القاهرة: دار النهضة العربية.

17. حسني، محمود نجيب(1964)، المجرمون الشواذ، ط2، القاهرة.

18. حسني، محمود نجيب(1988)، شرح قانون العقوبات، القسم الخاص، القاهرة: دار النهضة العربية.

19. حسني، محمود نجيب(1989)، شرح قانون العقوبات، القسم العام، القاهرة: دار النهضة العربية، 1985.

20. خريسات، صالح(2006/2005)، الآليات الدولية لمقاومة الإرهاب بعد احداث 11 أيلول 2001م، رسالة ماجستير، جامعة عمان العربية.

21. الخليل، عماد علي(2000)، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت: دراسة علمية في ظل أحكام قانون العقوبات الأردني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 مايو 2000.

22. الخييلي، أحمد(2006)، غسيل الأموال عبر الانترنت، رسالة دكتوراة، جامعة عمان العربية للدراسات العليا.

23. داود، حسن طاهر(2000)، جرائم نظم المعلومات، ط1، الرياض: أكاديمية نايف للعلوم الأمنية.

24. راشد، علي(1974)، القانون الجنائي، المدخل واصول النظرية العامة، ط2، القاهرة: دار النهضة العربية القاهرة
25. رستم، هشام محمد فريد(1994)، قانون العقوبات ومخاطر تقنية المعلومات، اسيوط: مكتبة الآلات الحديثة.
26. رستم، هشام محمد فريد(2000)، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة.
27. الرومي، محمد أمين(2003)، جرائم الكمبيوتر والإنترنت، الإسكندرية: دار المطبوعات الجامعية.
28. الزيدي، وليد (2003) القرصنة على الإنترنت الحاسوب والتشريعات القانون عمان. دار أسامة للنشر.
29. سايمون كولن، التجارة على الإنترنت، ترجمة: يحيى مصلح، بيت الأفكار الدولية، الولايات المتحدة الامريكية، 1999.
30. سرور، أحمد فتحي سرور(1985)، الوسيط في قانون العقوبات ، القسم الرابع، ط4، القاهرة: دار النهضة العربية
31. سلامه، محمد عبد الله أبو بكر(2006)، جرائم الكمبيوتر والانترنت، الاسكندرية: منشأة المعارف.
32. السماك، محمد (1992)، الإرهاب والعنف السياسي، بيروت: دار النقاش للطباعة والنشر والتوزيع.
33. السماك، محمد(1992)، الإرهاب والعنف السياسي، بيروت: دار النفائس للطباعة والنشر والتوزيع.
34. السند، عبدالرحمن بن عبدالله(2004)، وسائل الإرهاب الإلكتروني عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها،

جامعة الإمام محمد بن سعود الإسلامية، المملكـــة العربية السعوديـــة، المؤتمر العالمي عن موقف الإسلام من الإرهاب،1425هـــ.

35. شريف، حسين(1997)، الإرهاب الدولي وانعكاساته خلال أربعين قرناً، ج1، القاهرة: الهيئة المصرية العامة للكتاب.

36. شكور، جليل وديع(1997)، العنف والجريمة، بيروت: الدار العربية للعلوم.

37. شلالا، نزيه نعيم(2003)، الإرهاب الدولي والعدالة الجنائية، ط1، بيروت: منشورات الحلبي.

38. الشوا، محمد سامي(1998)، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط2، القاهرة: دار النهضة العربية.

39. الشوا، محمد سامي(1998)، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط2، القاهرة: دار النهضة العربية.

40. الشوا، محمد(2001)، السياسة الجنائية في مواجهة غسيل الأموال، القاهرة: دار النهضة العربية.

41. الشوابكة، محمد أمين(2004)، جرائم الحاسوب والإنترنت، عمان: دار الثقافة للنشر والتوزيع.

42. صالح، نايل عبد الرحمن(1998)، الجريمة المنظمة، بحث مقدم في ندوة: الجريمة المنظمة عبر الحدود العربية، الأمانة العامة لوزراء العدل العرب لعام 1998، مجلة السياسة الدولية، العدد 135.

43. صدقي، عبد الرحيم(1985)، الإرهاب السياسي والقانون الجنائي، القاهرة: دار النهضة العربية.

44. الصغير، جميل عبدالباقي(1999)، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، ط1، القاهرة: دار النهضة العربية.

45. العازمي، خالد(2007)، جريمة الإرهاب في التشريع الكويتي، دراسة مقارنة، كلية الحقوق، جامعة عمان العربية.

46. عالية، سمير(1996)، أصول قانون العقوبات، بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع.
47. عبد الحميد، احمد(1999)، التعاون الأمني العربي والتحديات الأمنية، الرياض: أكاديمية نايف للعلوم الأمنية.
48. عبد المطلب، ممدوح عبدالحميد(2000)، جرائم استخدام شبكة المعلومات العالمية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 مايو 2000.
49. عبيد، حسنين(1997)، الجريمة الدولية، ط1، القاهرة: دار النهضة العربية، القاهرة.
50. عرب، يونس(2002)، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، ط1، منشورات إتحاد المصارف العربية.
51. عرب، يونس(2006)، صور الجرائم الإلكترونية واتجاهات تبويبها ورقة عمل في: مؤتمر تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، ورشة عمل، هيئة تنظيم الاتصالات، مسقط – سلطنة عمان، 2-4 نيسان / ابريل 2006.
52. العفيف، محمد عبد الكريم(2011)، جرائم الإرهاب في قانون العقوبات الأردني، رسالة دكتوراة، كلية الحقوق، جامعة عمان العربية.
53. عفيفي، كامل عفيفي(2003)، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، بيرون: منشورات الحلبي الحقوقية.
54. علوان، حسن(2008)، موضوعة الإرهاب في الفضائيات العربية، أطروحة دكتوراة، الدنمارك: كلية الآداب والتربية، الأكاديمية العربية المفتوحة في الدنمارك.
55. العناني، ابراهيم(1992)، النظام الدولي الأمني، مجلة العلوم القانونية والاقتصادية، ع2، س34.

56. عوض، أسامة محي الدين (1993)، جرائم الكمبيوتر والإنترنت والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي.

57. الفتلاوي، سهيل(2005)، الإرهاب والإرهاب المضاد، ط1، بيروت: دار الفكر العربية.

58. قشقوش، هدى(1993)، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان: الجرائم الواقعة في مجال تكنولوجيا المعلومات، القاهرة 25-28 أكتوبر، القاهرة: دار النهضة العربية.

59. قريني علي، عادل يحيى(2000)، النظرية العامة للأهلية الجنائية، القاهرة: دار النهضة العربية.

60. القهوجي، علي عبد القادر(1992)، الحماية الجنائية لبرامج الحاسب، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الأسكندرية، عدد 24.

61. كوفال . م(1995)، الاوجه المتعددة للإرهاب، القاهرة: الدار العربية للكتاب.

62. الكيلاني، هيثم(1997)، الإرهاب يؤسس دولة، دار الشروق.

63. لطفي، محمد حسام (1993)، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم إلى مؤتمر السادس للجمعية المصرية للقانون الجنائي.

64. مجلة السياسة الدولية(نيسان 1993)، الإرهاب والسياسة الدولية، العدد112، القاهرة: دار الاهرام.

65. مجمع الفقه الإسلامي الدولي(ذي القعدة من عام 1423ه)، قرار دورته الرابعة عشرة، الدوحة.

66. المجمع الفقهي لرابطة العالم الإسلامي(1422هــ)، بيان مكة المكرمة الصادر، الدورة السادسة عشرة، مكة المكرمة: رابطة العالم الإسلامي.

67. المراغي، محمود (2002)، حرب الجلباب والصاروخ وثائق الخارجية الأمريكية حول الإرهاب، القاهرة: دار الشروق.
68. مصطفى، محمود(1983)، شرح قانون العقوبات القسم العام، القاهرة: دار النهضة العربية.
69. مورجان . ك(1989)، الإرهاب والعنف، مترجم عن الانكليزية، القاهرة: الدار العربية للكتاب.
70. ميلاد، ميلاد(2007)، جريمة اتلاف نظم المعلومات، رسالة ماجستير، كلية الحقوق، جامعة عمان العربية.
71. نايل، ابراهيم عبد(1996)، السياسة الجنائية في مواجهة الإرهاب، دار النهضة العربية، القاهرة.
72. نجم، محمد صبحي(2000)، قانون العقوبات القسم العام، عمان: دار الثقافة للنشر والتوزيع، عمان.
73. نظمي، رانيا(2010)، الفراغ الفكري وتأثيراته على الاستخدام السيئ لتقنية الاتصالات الحديثة، مؤتمر الإرهاب بين تطرف الفكر وفكر التطرف، الجامعة الاسلامية بالمدينة المنورة.
74. النوايسة، عبدالاله(2005)، الجرائم الواقعة على امن الدولة في التشريع الأردني، عمان: دار وائل للنشر والتوزيع.
75. هروال، نبيلة (2007)، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الاسكندرية: دار الفكر الجامعي.

القوانين والاتفاقيات والمواثيق الدولية

1. قانون العقوبات الاردني رقم 16 لسنة 1960

2. مجموعة من قرارات مجلس الامن: http://www.oppc.pna.net/mag/mag3/p18-3.htm
3. الاتفاقية الأوروبية لقمع الإرهاب 1977.
4. الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998.
5. الاتفاقية العربية لمكافحة الإرهاب لعام 1988.
6. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012.
7. اتفاقية لاهاي 1970 الخاصة بقمع الاستيلاء غير المشروع على الطائرات.
8. اتفاقية نيويورك لحماية الأشخاص المتمتعين بحماية دولية لعام 1973.
9. الأمانة العامة لمجلس وزراء الداخلية العرب، مدونة قواعد السلوك للدول الأعضاء بمجلس وزراء الداخلية العرب لمكافحة الإرهاب، تونس، 1996.

مواقع الانترنت

1. الألفي، محمد محمد (2005)، جرائم التجسس والإرهاب الإلكتروني عبر الانترنت، منشور في موقع منتدى المحامين العرب على الرابط: http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=36212&Type=3
2. باكير، علي حسين(2010)، الحروب الإلكترونية في القرن الـــ21، منشور في مركز الجزيرة للدراسات على الرابط:http://errorpage.aljazeera.net
3. شبكة الإعلام العربي http://www.moheet.com/show_files.aspx?fid=137476:

4. الدغيلبي، محمد(2012)، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012، خبر منشور في صحيفة الرياض، العدد 16012، تاريخ 2012/4/26، موقع الصحيفة على الرابط: http://www.alriyadh.com/2012/04/26/article730586.html
5. خبر بعنوان، كتيبة عسكرية لمكافحة الإرهاب الإلكتروني، منشور في موقع شبكة وساحات عيون العرب على الرابط: http://vb.arabseyes.com/t94470.html
6. خبر منشور في موقع الجزيرة نت على الرابط: http://www.aljazeera.net/news/pages/e1d449d4-2f7f-4b39-b838-3f161adc8545
7. التوقيع على الاتفاقية الدولية لمكافحة الإرهاب عبر الإنترنت، 2001/11/23، خبر منشور في موقع الجزيرة نت على الرابط:-http://www.aljazeera.net/news/pages/e1d449d4-2f7f-4b39-b838-3f161adc8545
8. العالي، عادل محمد العيد، الشباب والانترنت: http://www.mlathat.net/vb/showthread.php?p=6417.
9. الصيفي، صلاح(2008)، مقال بعنوان"الإرهاب الإلكتروني ... وحش جديد يصعب اصطياده "، منشور في موقع آفاق على الرابط: http://www.aafaq.org/malafat.aspx?id_mlf=43
10. العادلي، محمود صالح (2009)، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، بحث منشور في منتدى الدكتورة شيماء عطا الله على الانترنت: http://www.shaimaaatalla.com/vb/showthread.php?t=4377
11. المصري، مهران زهير(2011)، الإرهاب الإلكتروني، منشور في موقع مجلة الباحثون الإلكتروني مجلة علمية فكرية ثقافية شهرية، على الرابط: http://albahethon.com/?page=show_det&id=1320
12. مجلس الوزراء يوافق على اتفاقية مكافحة غسل الأموال وتمويل الإرهاب لسنة2012، خبر منشور في موقع محطة الحقيقة الدولية بتاريخ 2012/2/23 على الرابط: http://factjo.com/pages/newsdetails.aspx?id=12534

13. مجلة بريس المغرب الإلكترونية، مقال بعنوان الإرهاب الإلكتروني، منشور على الرابط: http://press.marocs.net/t398-topic

14. عطية، عمرو(د.س)، إسرائيل رئيساً لفريق مكافحة الإرهاب الإلكتروني في إسرائيل، خبر منشور في صحيفة الوسط الإلكترونية، http://www.el-wasat.com/portal/News-55614215.html

15. النابلسي، محمد أحمد(2011)، الإرهاب الإلكتروني يهدد أمريكا، منشور في موقع المركز العربي للدراسات المستقبلية على الانترنت، 2011/11/21، على الرابط: http://www.mostakbaliat.com/?p=14223

المراجع الاجنبية:

1. Cyber Security Strategy of the United Kingdom، UK، June 2009، available at:www.cabinetoffice.gov.uk/media/216620/css0906.pdf
2. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure ،The White House، available at:www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
3. Cyberterrorism-testimony before the U.S.House of respresentatives by: Dr. Dorothy E Dening، Georgetown Uni. May 23، 2000، available at:http://www.cs.geoegetown.edu/~denning
4. Elinor Sloan، 2010، p: 8.، available at: www.cdfai.org/PDF/China%20Strategic%20Behaviour.pdf
5. Gina de Angelis; Syber Crimes، by Chelsa house publisher، USA، 2000
6. Lee Smith، Does Stuxnet Mean Cyberwar?، available at:www.weeklystandard.com/blogs/does-stuxnet-mean-cyberwar
7. M . Cherif Bassioni . Prop lems of media coverage of nonstate –Sponsonad terror Wilnnington . 1983
8. Mark Clayton، Staff writer، Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant، 2010، available at:http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant
9. Robert knake، Richard A. Clarke، Cyber War، HarperCollins، 2010.
10. Robert McMillan، Was Stuxnet Built to Attack Iran's Nuclear rogram?،2010، Available

at:www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_a
ttack_irans_nuclear_program.html

***الرد على ملاحظات لجنة المناقشة*:**

ارجو ان ابين ما قمت به من تعديلات واجراءات على اطروحتي الموسومة بـــــ: "الارهاب في الفضاء الالكتروني" بعد ملاحظات لجنة المناقشة كالآتي:

أ. قامت الباحثة بالتصدي للركن الشرعي (نصوص التجريم) في الصفحات 138-146 من الاطروحة.

ب. قامت الباحثة بإبراز نماذج (صور) متعددة من جريمة الارهاب الالكتروني او ما يمكن توافره من جرائم الكترونية في سياق ارتكاب جرائم الارهاب الالكتروني بالتوافق مع الملاحظة رقم 2 من تقرير اللجنة.

ج. قامت الباحثة بتوضيح علاقة بعض الجرائم بالارهاب الالكتروني كجريمة الذم والقدح بالرغم من عدم وجود ارتباط بينها وبين جريمة الارهاب الالكتروني ودون الخوض بتفاصيل الا انها اشارت الى ذلك وبينت انها غير ذات صلة الا انها قد تصاحب جريمة الارهاب الالكتروني لا أكثر، وأنها لا ترقى بأي حال الى مستوى الجريمة الارهابية.

د. تم اجراء تعديلات التوثيق بما يتفق مع ملاحظة اللجنة.

ه. تم ابراز شخصية الباحثة في كثير من مواضع الدراسة.

و. جرى اقتراح نص في التوصيات، وتقديم مقترحات لسد النقص في التشريع الاردني بخصوص الجرائم الالكترونية.

ز. تم اثراء الاطروحة بالاجتهادات القضائية ما أمكن لقلة القرارات في هذا الصدد.

ح. تم مراعاة التوازن بين الفصول ما أمكن.

ط. تم ابراز التطور التشريعي للارهاب في الاردن في الصفحات 138 وما بعدها.

ك. تم ما أمكن ابراز العلاقة بين التشريعات الوطنية والمعاهدات الدولية ذات الشأن.

ل. تم ترقيم الفهرس وتعديله.